
**UNIVERSIDAD DE GUAYAQUIL**

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

# IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A.

**PROYECTO DE TITULACIÓN**

Previa a la obtención del Título de:

**INGENIERO EN NETWORKING Y TELECOMUNICACIONES**

**AUTOR:**

EDWIN EDUARDO SÁNCHEZ ESTRADA

**TUTOR:**

ING. DÉBORA KAYANA PRECIADO MAILA, M.SC.

GUAYAQUIL – ECUADOR

2017

| REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA | | | | |
|---|---|---|---|---|
| FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN | | | | |
| **TÍTULO:** | IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A. | | | |
| **AUTOR:** | EDWIN EDUARDO SÁNCHEZ ESTRADA | | | |
| **TUTOR:** .<br>**REVISOR:** | Ing. Débora Preciado Maila MSc<br>Ing. Ángel Ochoa Flores MSc. | | | |
| **INSTITUCIÓN:** | Universidad de Guayaquil | | | |
| **UNIDAD/FACULTAD:** | Facultad de Ciencias Matemáticas y Físicas | | | |
| **MAESTRÍA/ESPECIALIDAD:** | Carrera de Ingeniería en Networking y Telecomunicaciones | | | |
| **GRADO OBTENIDO:** | Ingeniero en Networking y Telecomunicaciones | | | |
| **FECHA DE PUBLICACIÓN:** | | **No. DE PÁGINAS:** | | |
| **ÁREAS TEMÁTICAS:** | Redes | | | |
| **PALABRAS CLAVES /KEYWORDS:** | VPN, Latch, seguridad, encriptación, SSH<br>VPN. Latch, security, encryption, SSH | | | |


**RESUMEN/ABSTRACT:**

Hoy en día la confidencialidad, integridad y disponibilidad de la información se ha visto afectada por los crackers que realizan ataques cibernéticos interceptando los datos de los usuarios cuando se conectan a una red inalámbrica pública o con bajo nivel de seguridad, además los usuarios no tienen conciencia de los riesgos y amenazas a los que están expuestos conectándose a estas redes; pudiéndose dar ataques de suplantación de identidad por robo de credenciales, fraudes electrónicos o extracción de información sensible en casos de ambientes empresariales Los sistemas de redes virtuales privadas (VPN), nos aportan con la conexión segura a la red de datos por medio de un túnel de cifrado donde nuestra información de carácter sensible estará salvaguardada ante posibles ataques de intercepción e infiltración de datos confidenciales donde estos ataques son gestionados por los crackers para la suplantación de identidad. Estos sistemas beneficiaran a muchos usuarios que intenten realizar transacciones comerciales, registros en páginas o inicios de sesión en sus redes sociales, o en aplicativos propios de la empresa desde una red distinta.

Today, the confidentiality, integrity and availability of information has been affected by crackers that perform cyber-attacks by intercepting user data when they connect to a public or low-security wireless network, and users are not aware of the risks and threats to which they are exposed by connecting to these networks; being able to give impersonation attacks by theft of credentials, electronic frauds or extraction of sensitive information in cases of business environments The systems of virtual private networks (VPN), contribute to us with the secure connection to the network of data by means of a tunnel encryption where our sensitive information will be safeguarded against possible interception and infiltration of sensitive data where these attacks are managed by the crackers for phishing. These systems will benefit many users who attempt to conduct business transactions, page registrations or logins on their social networks, or in company-owned applications from a different network.


| | | | | |
|---|---|---|---|---|
| **ADJUNTO PDF:** | | | | |
| **CONTACTO CON AUTOR/ES:** | Teléfono: | 0996397671 | E-mail | edwin.sancheze@ug.edu.ec |
| **CONTACTO CON LA INSTITUCIÓN:** | Nombre: | Secretaría de la Facultad | | |
| | Teléfono: | 042307729 | | |
| | E-mail: | juan.chaveza@ug.edu.ec | | |

## CARTA DE APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación, "**Implementación de un servidor OpenVPN integrado con seguridad Latch montado en una Raspberry PI para la empresa Reporne S.A.**" elaborado por el Sr. EDWIN EDUARDO SÁNCHEZ ESTRADA **alumno no titulado** de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

**Atentamente**

**Ing. Débora Preciado Maila MSc.**

**TUTOR**

## DEDICATORIA

Dedico el presente proyecto a Dios todopoderoso quien ha guiado mi camino y me permitió culminar esta etapa de mi vida. A mi madre Amelia, quién ha sido pilar fundamental en mi vida, por sus consejos, dedicación y enseñarme valores y a nunca rendirme. A mi hermana Gabriela quién también ha sido mi mejor amiga. A mi hijo Mateo quién es la fuerza que me motiva cada día a ser mejor y esforzarme más. A mi esposa Sofía e hijas quienes me han ayudado y apoyado a culminar este objetivo, desde el inicio hasta su presentación final.

**Edwin Sánchez Estrada**

## AGRADECIMIENTO

Agradezco a los docentes que me prepararon todo este tiempo de mi carrera, a mis amigos con los que hemos compartido gratos momentos dentro y fuera de la universidad, a mi familia que siempre ha estado junto a mí apoyándome y dándome ánimos para no rendirme. Le agradezco a mi tutora Ing. Débora Preciado Maila quien me guio durante todo este proceso y quien siempre me dio su total apoyo. ¡Gracias a todos!

**Edwin Sánchez Estrada**

## TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, MSc.
DECANO DE LA FACULTAD
CIENCIAS MATEMÁTICAS Y FÍSICAS

Ing. Harry Luna Aveiga, MSc.
DIRECTOR
INGENIERIA EN NETWORKING Y
TELECOMUNICACIONES

Ing. Débora Preciado Maila, MSc
PROFESOR DIRECTOR
DEL PROYECTO DE TITULACIÓN

Ing. Ángel Ochoa Flores, MSc.
PROFESOR TUTOR REVISOR
DEL PROYECTO DE TITULACIÓN

Ab. Juan Chávez Atocha
SECRETARIO

## DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Titulación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL"

**EDWIN EDUARDO SÁNCHEZ ESTRADA**


UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

**CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**

# "IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A."

Proyecto de Titulación que se presenta como requisito para optar por el título de
**INGENIERO EN NETWORKING Y TELECOMUNICACIONES**

**Autor:** EDWIN EDUARDO SÁNCHEZ ESTRADA

C.I. 0923159594

**Tutor**: ING. DÉBORA PRECIADO MAILA, MSc.

Guayaquil, 12 de diciembre de 2017

## CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

**CERTIFICO:**

Que he analizado el Proyecto de Titulación presentado por el estudiante EDWIN EDUARDO SÁNCHEZ ESTRADA, como requisito previo para optar por el título de Ingeniero en Telecomunicaciones y Networking, cuyo tema es:

**"IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A"**

Considero aprobado el trabajo en su totalidad.

Presentado por:

Edwin Eduardo Sánchez Estrada Cédula de ciudadanía N° 092315959-4

Tutor: Ing. Débora Preciado Maila, MSc.

Guayaquil, 12 de diciembre de 2017

**UNIVERSIDAD DE GUAYAQUIL**
**FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS**
**CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**

**Autorización para Publicación de Proyecto de Titulación en Formato Digital**

**1. Identificación del Proyecto de Titulación**

| | |
|---|---|
| **Nombre Alumno:** Edwin Eduardo Sánchez Estrada | |
| **Dirección:** Cdla. Villamil Mz. E V. 11 | |
| **Teléfono:** 0996397671 | **E-mail:** edwin.sancheze@outlook.com |

| |
|---|
| **Facultad:** Ciencias Matemáticas y Físicas |
| **Carrera:** Ingeniería en Networking y Telecomunicaciones |
| **Título al que opta:** Ingeniero en Networking y Telecomunicaciones |
| **Profesor guía:** Ing. Débora Preciado Maila, MSc. |

| |
|---|
| **Título del Proyecto de titulación:** "IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A" |

| |
|---|
| **Tema del Proyecto de Titulación:** VPN, Latch, Seguridad, Encriptación, SSH. |

**2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación**

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

**Publicación electrónica:**

| | | | |
|---|---|---|---|
| Inmediata | **x** | Después de 1 año | |

Firma Alumno:

**3. Forma de envío:**

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y .Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

DVDROM [ ] CDROM [ ]

# INDICE GENERAL

## ABREVIATURAS

| | |
|---|---|
| **VPN** | Virtual Private Network |
| **bps** | Bits por segundo |
| **TCP** | Transmission Control Protocol |
| **IP** | Internet Protocol |
| **NSFNET** | National Science Foundation's Network |
| **IrDA** | Infrared Data Association |
| **USB** | Universal Serial Bus |
| **ISP** | Internet service provider |
| **PPTP** | Point to Point Tunneling Protocol |
| **IPsec** | Internet Protocol security |
| **SSL** | Secure Sockets Layer |
| **PPP** | Point-to-Point Protocol |
| **GRE** | Generic Routing Encapsulation |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IETF** | Internet Engineering Task Force |
| **OSI** | Open Systems Interconnection |
| **UDP** | User Datagram Protocol |
| **L2TP** | Layer 2 Tunneling Protocol |
| **ESP** | Encapsulating Security Payload |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **TLS** | Transport Layer Security |

| | |
|---|---|
| **HMAC** | Hash-based message authentication code |
| **CPU** | Central processing unit |
| **PDU** | Protocol data unit |
| **MD5** | Message-Digest Algorithm 5 |
| **NAT** | Network Address Translation |
| **ARM** | Advanced RISC Machine |
| **SBC** | Single Board Computer |
| **BLE** | Bluetooth Low Energy |
| **GPIO** | General Purpose Input/Output |
| **CSI** | Camera Serial Interface |
| **DSI** | Display Serial Interface |
| **NTFS** | New Technology File System |
| **RISC** | Reduced instruction set computing |
| **CISC** | Complex instruction set computing |
| **TOTP** | Time-based One-time Password Algorithm |

## SIMBOLOGÍA

| | |
|---|---|
| **S** | Desviación estándar |
| **e** | Error |
| ***E*** | Espacio muestral |
| **E(*Y*)** | Esperanza matemática de la v.a. y |
| **s** | Estimador de la desviación estándar |
| **e** | Exponencial |

# ÍNDICE DE CUADROS

**Pág.**

# ÍNDICE DE GRÁFICOS

**Pág.**

**UNIVERSIDAD DE GUAYAQUIL**

**FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS**

**CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**

# "IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A."

Autor: Edwin Sánchez Estrada

Tutor: Ing. Débora Preciado, MSc.

## Resumen

Hoy en día la confidencialidad, integridad y disponibilidad de la información se ha visto afectada por los crackers que realizan ataques cibernéticos interceptando los datos de los usuarios cuando se conectan a una red inalámbrica pública o con bajo nivel de seguridad, además los usuarios no tienen conciencia de los riesgos y amenazas a los que están expuestos conectándose a estas redes; pudiéndose dar ataques de suplantación de identidad por robo de credenciales, fraudes electrónicos o extracción de información sensible en casos de ambientes empresariales Los sistemas de redes virtuales privadas (VPN), nos aportan con la conexión segura a la red de datos por medio de un túnel de cifrado donde nuestra información de carácter sensible estará salvaguardada ante posibles ataques de intercepción e infiltración de datos confidenciales donde estos ataques son gestionados por los crackers para la suplantación de identidad. Estos sistemas beneficiaran a muchos usuarios que intenten realizar transacciones comerciales, registros en páginas o inicios de sesión en sus redes sociales, o en aplicativos propios de la empresa desde una red distinta.

**UNIVERSIDAD DE GUAYAQUIL**

**FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS**

**CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**

# "IMPLEMENTATION OF AN OPENVPN INTEGRATED SERVER WITH SECURITY LATCH MOUNTED IN A RASPBERRY PI FOR THE COMPANY REPORNE S.A."

Author: Edwin Sánchez Estrada

Advisor: Ing. Débora Preciado, MSc.

## Abstract

Today, the confidentiality, integrity and availability of information has been affected by crackers that perform cyber-attacks by intercepting user data when they connect to a public or low-security wireless network, and users are not aware of the risks and threats to which they are exposed by connecting to these networks; being able to give impersonation attacks by theft of credentials, electronic frauds or extraction of sensitive information in cases of business environments The systems of virtual private networks (VPN), contribute to us with the secure connection to the network of data by means of a tunnel encryption where our sensitive information will be safeguarded against possible interception and infiltration of sensitive data where these attacks are managed by the crackers for phishing. These systems will benefit many users who attempt to conduct business transactions, page registrations or logins on their social networks, or in company-owned applications from a different network.

# INTRODUCCIÓN

La comunicación es uno de los pilares fundamentales en la evolución de la sociedad; por ello, en el campo empresarial, es importante estar informado sobre los temas que acontecen en la misma, sobre un cambio de directriz, creación de nuevas métricas, inconvenientes con los clientes y manejo de requerimientos de manera oportuna.

Mediante el siguiente proyecto se propone la implementación una red privada virtual que permita la interconexión de equipos en sitios remotos hacía la red empresarial, de manera simple, segura, rápida y confiable; utilizando como medio el Internet y aplicado únicamente a dispositivos y equipos autorizados previamente por el departamento IT de la empresa.

Para la creación de dicha red privada virtual o VPN se utilizará el software libre OpenVPN que se implementará como servidor dentro de un dispositivo compacto denominado Raspberry Pi. De esta manera se economizará en la compra de hardware de un equipo con características de servidor y con el uso de aplicaciones de código abierto.

La empresa Reporne S.A. actualmente no cuenta con una solución que permite a sus colaboradores que se encuentren fuera de la misma, por motivos estrictamente laborales, conectarse a la empresa para gestionar tareas concernientes a sus actividades diarias o acerca de asuntos emergentes que se puedan suscitar durante su ausencia.

Al utilizar la VPN el colaborador tendrá acceso a realizar consultas en los aplicativos internos facilitados por la empresa, conectarse de manera remota a equipos previamente autorizados, utilizar la red VoIP perteneciente a la corporación, tener acceso al servidor de correo electrónico empresarial, entre otros.

En el primer capítulo se indicará la problemática presentada, objetivo general y específicos que se lograrán con la implementación del presente proyecto, el alcance y la justificación por la cual se propuso la realización del mismo en la empresa Reporne S.A.

En el segundo capítulo se detallan la fundamentación teórica sobre los diferentes recursos de hardware y software que se utilizarán, acerca de las redes VPN, el servicio OpenVPN y la aplicación Latch; además sobre la fundamentación legal que se emplea según las leyes y estatutos existentes, códigos integrales y normativas, tanto nacionales como

internacionales. Se determinará la hipótesis a demostrar, las definiciones de concepto de los términos investigados dentro del capítulo.

En el tercer capítulo se define la metodología a utilizarse, la muestra y población que se estudiará, el tipo de investigación que se empleará; adicional se mostrarán la tabulación de la encuesta realizada al total de la población de los beneficiados y la validación de la hipótesis.

En el cuarto capítulo se desarrolla la propuesta, se detalla la factibilidad del proyecto y se generan las conclusiones y recomendaciones las cuales se basan en los objetivos planteados y los resultados obtenidos en la investigación y las pruebas realizadas.

# CAPÍTULO I

# EL PROBLEMA

## PLANTEAMIENTO DEL PROBLEMA

### Ubicación del Problema en un Contexto

La comunicación oportuna es una de las premisas que existen en las empresas para su crecimiento, sobre todo, cuando su núcleo de negocio son las transacciones en línea; cuando existe un problema que impide continuar con este esquema transaccional, conlleva a consecuencias negativas para el negocio, tales como: pérdida de dinero, desconfianza del cliente hacia la marca, baja competitividad ante otras empresas de recaudación, entre otras.

Reporne S.A., empresa domiciliada en Víctor Manuel Rendón y Córdova, Ed. Torres de la Merced, Piso 14 oficina 4, en la ciudad de Guayaquil, provincia del Guayas; constituida hace 18 años, está enfocada en ofrecer

a los habitantes de los sectores rurales, urbano-marginales y urbanos, servicios de recaudación y pagos, mediante diferentes instituciones; entre ellas: mutualistas, bancos, cooperativas, tiendas; ubicadas en sectores estratégicos, con la finalidad de facilitar al usuario final el pago a tiempo de sus facturas y obligaciones pendientes.

El departamento de IT para el monitoreo de los servidores transaccionales existe una red VPN sitio a sitio establecida, sin embargo, el uso de este servicio se limita a los equipos que se encuentran dentro de la oficina; en caso de existir caídas, no existe posibilidad de dicha área realice la gestión desde un punto remoto.

La empresa actualmente no posee una solución para los colaboradores que se encuentre de viaje por las diferentes reuniones, eventos y citas de negocio; pueda acceder a los diferentes aplicativos para revisión de transacción, generación de reportes y de interacción con los diferentes proveedores. De este modo, se crea una carga administrativa adicional para el personal encargado al cual se le solicita la generación de ciertos archivos, ya que existen otros, que, por su naturaleza, no pueden ser revisados por personas no autorizadas.

Con este proyecto se busca brindar acceso a los usuarios a la red corporativa de manera simple, rápida, pero sobre todo segura; para este fin será necesario únicamente tener un dispositivo con acceso a internet, poseer el aplicativo OpenVPN cliente instalado y que el computador haya sido previamente autorizado por el personal IT de la empresa. Una vez conectado, el equipo estará dentro de la red LAN desde el lugar remoto donde se encuentre.

**Situación Conflicto. Nudos Críticos**

La empresa Reporne S.A. tiene como aliados a 273 instituciones financieras, como Cooperativas y bancos; 380 centros autorizados de recaudación con cobertura de 1450 agencias en 472 localidades a nivel nacional, constituyéndose en un socio estratégico para el cobro y pago de diferentes servicios, permitiendo ampliar la red de manera integral aportando también al beneficio social.

Al existir diferentes proveedores y autorizadores (entidades que conectan a la empresa con proveedores sin convenio directo), se debe brindar seguimiento a las diferentes transacciones, eventos programados y no programados, y procesos que puedan afectar o variar en los diferentes productos, siendo la comunicación oportuna uno de los pilares fundamentales, que ha permitido a la empresa su expansión.

La implementación de esta herramienta, ayudará a que, aunque algún colaborador se encuentre de viaje por los diferentes menesteres que se puedan suscitar, esté siempre conectado a la red corporativa, y, sobre todo, estableciendo medidas de seguridad, evitando que terceros puedan acceder a manipular las transacciones que esta maneja lo cual podría derivar en robo de bases de datos o alteración de registros internos.

## Causas y Consecuencias del Problema

**CUADRO 1. CAUSAS Y CONSECUENCIAS DEL PROBLEMA**

| CAUSAS | CONSECUENCIAS |
|---|---|
| Conexión de usuarios desde fuera de la oficina inexistente | Envío de información a destiempo, no de primera mano. |
| Solicitud de reportes e informes a personal en oficina. | Carga administrativa adicional que genera retrasos en actividades recurrentes del personal |
| Problema en revisión de reportes confidenciales. | Deben ser revisados cuando el usuario regrese de su viaje. |
| Optimizar los tiempos de respuesta y solución. | Continuidad en el proceso operativo, generación oportuna de información sensible. |
| Aislamiento del servidor de correos interno | Falta de seguimiento a casos que se gestionan por correo electrónico |
| Afectación de productividad de usuarios | Retrasos en gestión y acumulación de trabajo |
| Desconexión del personal IT de la red corporativa | Retrasos en tiempos de solución en caso de afectaciones o dilatación de tiempo de entregables en proyectos |
| Inseguridad al realizar transacciones bancarias de la empresa en una red abierta | Robo de credenciales y datos bancarios corporativos |
| Falta de monitoreo de los servidores transaccionales | Pérdida de transacciones por falta de gestión para el restablecimiento de un servicio determinado |
| Incomunicación hacia la red VoIP (Telefonía IP) empresarial | Imposibilidad de llamar a usuarios telefónicamente en caso de no tener acceso celular o convencional |

**Elaboración:** Edwin Eduardo Sánchez Estrada
**Fuente:** Datos de la Investigación

**Delimitación del Problema**

El acceso remoto está orientado a mejorar la productividad de los usuarios que se encuentran fuera de la oficina; está dirigido especialmente al personal administrativo, sean estos gerentes, jefes, líderes y demás autorizados por el departamento IT. Esta implementación permitirá el acceso a la red corporativa para el uso de las aplicaciones internas, inclusive para la utilización de la herramienta 'escritorio remoto' hacia los equipos habilitados. La conexión se realizará por el aplicativo OpenVPN instalado en el host remoto, siendo este un software libre, basado en la arquitectura Cliente/Servidor, el cual permite establecer una red VPN mediante el servidor, que, en este caso, será una placa Raspberry Pi 3.

**CUADRO 2. DELIMITACIÓN DE LA INVESTIGACIÓN**

| Delimitación de la Investigación | |
|---|---|
| **Campo:** | Educación Superior |
| **Área:** | Herramientas código abierto |
| **Aspecto:** | Software OpenSource que permite a los usuarios conectarse a la red corporativa. |
| **Tema:** | Implementación de un servidor OpenVPN integrado con seguridad Latch montado en una Raspberry PI para empresa Reporne S.A. |
| **Geográfica:** | Reporne S.A.<br>Víctor Manuel Rendón y Córdova, Guayaquil. |
| **Espacio:** | 2017 |

**Elaboración:** Edwin Eduardo Sánchez Estrada
**Fuente:** Datos de la Investigación

## Formulación del Problema

Mediante la herramienta VPN se busca satisfacer la necesidad de estar conectado a la empresa para poder mantener la comunicación constante y actualizada a fin de mitigar problemáticas que puedan surgir cuando se deba estar ausente en la oficina, por requerimientos y exigencias del negocio. Actualmente la falta de este instrumento VPN para conectarse a la red corporativa cuando un colaborador no se encuentra en la oficina, dificulta el trabajo de los usuarios administrativos que buscan informar y resolver novedades de manera eficaz y eficiente, los problemas o métricas de la empresa.

¿Cómo incide la no implementación de una herramienta VPN cliente/servidor en el departamento administrativo?

¿Cómo incide la no implementación de una herramienta VPN cliente/servidor a los usuarios de la empresa Reporne S.A.?

## Evaluación del Problema

**Delimitado:** Basado en la implementación de una herramienta VPN para la empresa Reporne S.A.; abordando puntualmente el uso remoto de usuarios con cargos administrativos para su gestión regular y posibles eventos emergentes.

**Claro:** Se indicará paso a paso la aplicación de una red VPN mediante un servidor OpenVPN, donde se podrá instalar y configurar este servicio con las mejores prácticas sobre el tema de seguridad.

**Concreto:** Resolverá la problemática de acceso remoto a la red corporativa para usuarios, que, por tema de viajes laborales, deban estar ausentes de la empresa, a través de una herramienta VPN Cliente/Servidor la cual se explica de forma clara, directa y concisa para su posterior práctica en un ambiente de producción, facilitando el cumplimiento de las métricas de la empresa, para los beneficiarios antes mencionados.

**Relevante:** Esta implementación logrará mejorar la atención hacia los clientes internos y finales, ya que el proceso de comunicación y envío de información recurrente o emergente, no será interrumpido; generando resultados oportunos, evitando una mala percepción de la marca y de la empresa.

**Factible:** Es factible ya que cuenta con la aprobación para su implementación del personal IT de la empresa Reporne S.A. con el objetivo de ahorrar y optimizar recursos económicos, ya que existen las herramientas e infraestructura necesaria para su aplicación inmediata;

facilitando la interconexión con la red corporativa de los usuarios autorizados para este fin.

**Identifica los productos esperados:** Necesaria, debido a que actualmente los usuarios administrativos pierden su comunicación con la red empresarial cuando se encuentran fuera de la oficina generando retrasos en sus actividades y pérdida notable de productividad por su ausencia.

**Alcances del Problema**

- Implementación de un servidor OpenVPN en un dispositivo Raspberry Pi 3 con integración de seguridad adicional Latch.
- Establecer conexión con la red corporativa desde cualquier punto con acceso a internet mediante un túnel VPN.
- Habilitar/Deshabilitar a los usuarios que pueden acceder al servicio mediante el aplicativo Latch de Eleven Paths.
- Mantener el registro y control de las conexiones mantenidas con el servidor VPN.
- Validación de sitios web visitados mediante el servicio SniffVPN, el cual cotejará en VirusTotal para detectar si un sitio es seguro o malicioso.

## OBJETIVOS DE LA INVESTIGACIÓN

### Objetivo General

Implementar un servidor VPN con integración de seguridad Latch, montado en una Raspberry Pi para el cifrado de información por medio de un túnel de datos para la empresa Reporne S.A.

### Objetivos específicos

- Acceder a los equipos de la empresa mediante conexión remota, permitiendo trabajar desde cualquier equipo autorizado con conexión a Internet activa.
- Asegurar la comunicación entre un dispositivo externo autorizado y la red corporativa de la empresa Reporne S.A utilizando la herramienta Latch.
- Brindar la documentación necesaria para la creación de una red VPN sobre equipos Raspberry.

## JUSTIFICACIÓN E IMPORTANCIA DEL PROBLEMA

Es necesario realizar este trabajo de investigación para su posterior implementación, debido a que, aunque la empresa ya cuenta con Redes VPN, estas son peer-to-peer, es decir, que funcionan con equipos dentro de la empresa únicamente, limitando a los usuarios que no se encuentran en las instalaciones.

La implementación y posterior ejecución de este proyecto tiene como finalidad la continuidad de los diferentes procesos existentes en la compañía en sus diferentes áreas, los cuales son muy importantes al manejarse un ambiente transaccional, donde a cada segundo se realizan consultas, recaudaciones y reversos, y la respuesta oportuna para estos eventos es imprescindible; asimismo, permitirá la revisión de reportes e información sensible a la cual solo tiene acceso el personal con cargo administrativo, autorizado con antelación.

Debido a que el servidor OpenVPN será instalado dentro de una placa Raspberry PI, se ahorran costos, puesto que el valor entre este dispositivo y un equipo con características de servidor, es abismal; además se usará la misma estructura de la red y se añadirá como un servidor adicional a los ya existentes en la empresa.

Siendo esta una conexión VPN, cuenta con las seguridades necesarias para poder viajar por internet, no obstante, se agrega una capa adicional de protección para robustecer aún más la comunicación. La aplicación Latch, permite bloquear las conexiones que no se están utilizando para evitar usuarios malintencionados que tengan acceso a la PC autorizada; el administrador TI deberá habilitar la opción al usuario cuando este se encuentra fuera de la oficina y cuenta con el consentimiento respectivo para conectarse a la red remotamente.

De esta manera también se garantiza el acceso a poder revisar los servidores por parte del departamento de infraestructura y acceder a los diferentes recursos existentes por parte del área de desarrollo y de esta manera cumplir con los cronogramas establecidos para entregas de proyectos los cuales son indispensables para potencializar el crecimiento de la empresa, integrándola con más proveedores a nivel nacional.

# CAPÍTULO II

## MARCO TEÓRICO

En este apartado del capítulo se brindará la información necesaria para conocer los diferentes tipos de elementos que componen esta implementación, así mismo para que se pueda tener una visión más amplia de las tecnologías y protocolos utilizados con el objetivo de transmitir una fácil comprensión. El dispositivo y tecnología empleados se aplican actualmente en varios ámbitos, tanto corporativos, educativos, experimentales, ambientales, entre otros; ya que la comunicación oportuna, actualizada y segura es muy importante en la actualidad.

Este capítulo estará compuesto de cinco elementos que detallan y profundizan los tópicos acerca de este proyecto y de los recursos empleados.

1. **Antecedentes del estudio. -** Hace referencia a todos los trabajos investigativos previos que brindaron aporte al proyecto,

estableciendo pautas, sugerencias y mejoras, que permitirán el adecuado desarrollo del tema.

2. **Fundamentación teórica. -** Se indicarán los diferentes modelos y tipos de conexiones VPN utilizadas actualmente, desde su funcionamiento, diferencias en temas de complejidad y seguridad.
3. **Fundamentación social. -** Se explicará claramente de qué manera y a quiénes beneficiará este proyecto, bajo las políticas del buen vivir.
4. **Fundamentación legal. -** Se nombrarán las regulaciones, normativas y leyes existentes sobre el tema de seguridad de la información y sobre los diferentes delitos informáticos que pueden existir al acceder a una red no autorizada; también sobre las consecuencias legales para quienes las transgredan.

## ANTECEDENTES DEL ESTUDIO

Hasta hace poco tiempo, sólo las grandes empresas tenían la necesidad y los medios para conectar distintas sedes geográficamente. Inicialmente, se utilizaban enlaces punto a punto dedicado, los cuales acarreaban un alto costo y, entre más grande la distancia, más costosa era su implementación; cada sede funcionaba de manera independiente.

En la actualidad, cada vez son más las empresas que requieren conectarse con sedes nuevas ya que están en constante crecimiento, sin

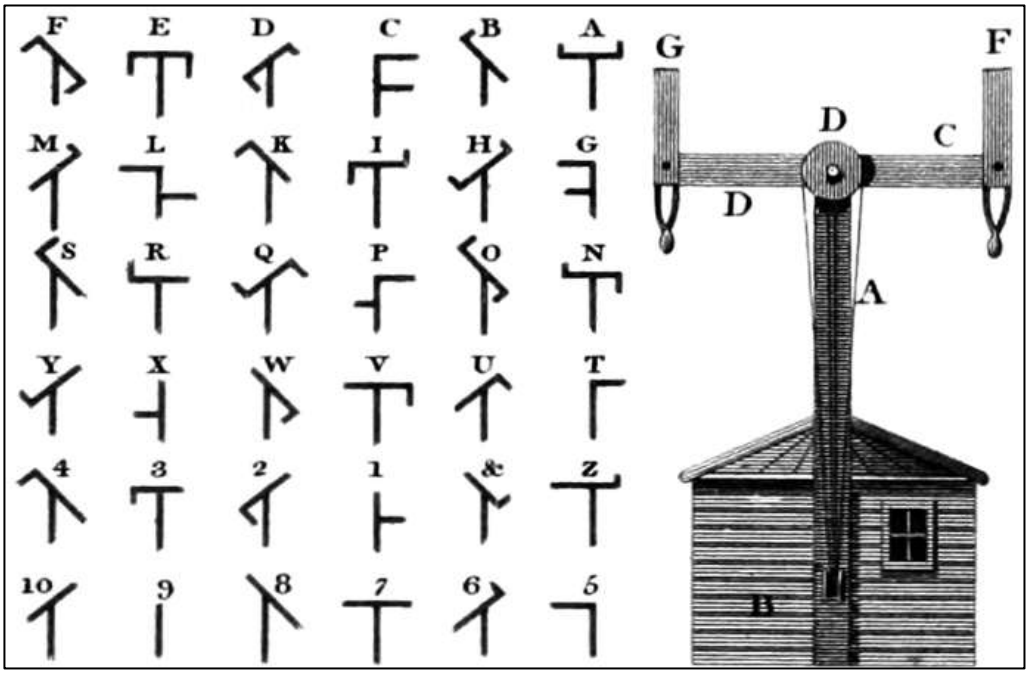
embargo, desean utilizar soluciones más económicas para poder afianzarse y poder seguir compitiendo en el mercado, sin dejar de lado la seguridad que requieren, tanto internamente, como para sus clientes, por lo cual se recurre a las conexiones mediante VPN.

## FUNDAMENTACIÓN TEÓRICA

### Historia de las Redes

Según la historia, las redes datan desde el siglo XIX, donde se produjo el primer intento de interconexión entre los países de Francia y Suecia, utilizando el telégrafo óptico para la comunicación. Esta técnica fue pionera de nuevas herramientas que surgieron para las transmisiones analógicas y digitales, entre ellas la recuperación de errores, compresión y codificación de información, por ejemplo. Las velocidades que oscilaban en ese entonces de unos 0.5 bps (bits por segundo), es decir unos 20 caracteres/minuto en promedio.

**GRÁFICO 1. TELÉGRAFO ÓPTICO**




**Fuente:** http://proyectoidis.org/claude-chappe/

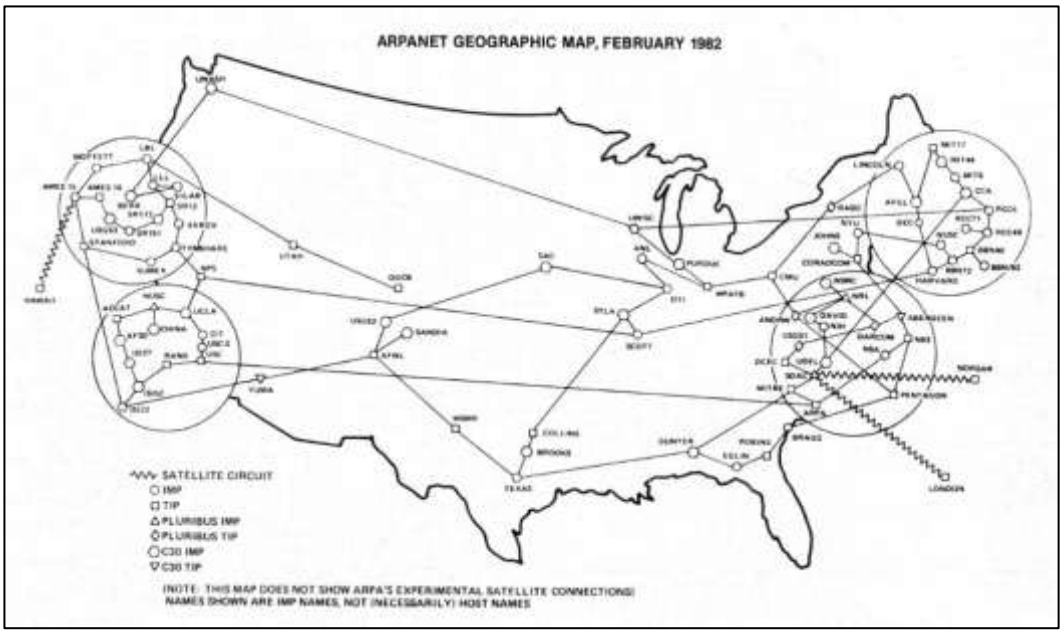
**Elaboración**: Edwin Sánchez Estrada

Luego llego Alexander Graham Bell a revolucionar el mundo de las comunicaciones con su invento, el teléfono, el cual funcionaba en sus inicios de manera centralizada donde los interesados recibían información a ciertas horas en el día bajo esta modalidad. Posteriormente se las implementó para las comunicaciones interpersonales, pero sin mayor relevancia. No obstante, su éxito se dio cuando existió en Boston un choque de trenes, donde se empleó este invento para localizar a doctores para que acudan a dicho accidente a socorrer a las víctimas.

Desde ese entonces, las comunicaciones han ido avanzando de manera vertiginosa en el globo, hasta que en 1969 la ARPANET, propiedad del

Departamento de Defensa de los Estados Unidos (DOD), puso en marcha la primera red de computadoras en Estados Unidos la cual permitía la interconexión del país anglosajón de costa a costa.

**GRÁFICO 2. RED ARPANET, FEBRERO 1982**




**Fuente:** https://www.vox.com/a/internet-maps/

**Elaboración:** Edwin Sánchez Estrada

En los años 80, se financiaron varios centros de supercomputación dentro de EEUU y en 1986 se creó la NSFNET, una red basada en TCP/IP, con el fin de vincular estos centros y dar acceso a los investigadores de dicho país para su uso. Luego de ello, se ampliaron los alcances, permitiendo utilizar dicha red para objetivos académicos; por ello, se convirtió en la

columna para el resto de redes que fueron creadas como regionales, tanto dentro como fuera de Estados Unidos.

En el año 1993, el termino Internet fue denominado por los Estados Unidos como como una red totalmente global, también denominada World Wide Web. A partir del 2000, el Internet ha ido creciendo exponencialmente, conectando a todos los rincones del mundo, indiferentemente del continente al que pertenezca el usuario, sin embargo, para que esta gran red exista, se debieron sectorizar y regularizar las subredes que la componen, para evitar la desorganización que acarreaba este crecimiento acelerado, para ello se procedió a clasificarlas.

**Clasificación de las redes**

Las redes tienen varias clasificaciones, sin embargo, se hablará en este trabajo de dos grupos especialmente: Redes por su alcance y redes por su pertenencia.

**Redes por su alcance**

Se clasifican en:

**PAN. –** son redes que cubren un área reducida, como el comedor de una casa o habitación. La más comercial y conocida en este ámbito es el

Bluetooth y las IrDA, en su versión Wireless (WPAN) y el USB (Universal Serie Bus) y FireWire en cableado (Mansilla, 2014, p. 4). Dichas redes por lo general conectan dispositivos como parlantes, audífonos, impresoras, etc.

**LAN. –** estas redes son de área local, existen tanto cableadas (Redes Ethernet) tanto como inalámbricas (Wireless LAN); por lo general son utilizadas en oficinas o empresas, estas son denominadas como grupos de trabajo (Mansilla, 2014, p. 4); también se utilizan en hogares.

**MAN. –** es conocida como Red de Área Metropolitana, permite la conexión de distintos puntos dentro de una misma área metropolitana; de allí su nombre. Se encuentran entre los parámetros de una red LAN y una red WAN; esta red no se extiende fuera de los límites de una urbe (Mansilla, 2014, p. 4). Un ejemplo claro sería una conexión entre el norte y sur de la ciudad de Guayaquil.

**WAN. –** Una Red de Área Extendida, por su traducción al español, es la que abarca un espacio mucho más amplio, geográficamente hablando, para ello se pueden citar las redes satelitales o el Internet, que permite conectar diferentes países, inclusive diferentes continentes. Sus medios más utilizados para este fin son la fibra óptica y los satélites de comunicaciones.

**Virtual private network (VPN). –** son un sistema de conectividad que permite crear conexiones virtuales con acceso remoto a recursos

específicos, siendo esta una ampliación segura y económica de una red LAN sobre una red pública no controlada como lo es el Internet (Alvarez, Jorquera, Sepúlveda, & Zamora, 2014). En la actualidad, el uso más habitual es para Intranet de redes corporativas, repositorios de archivos y uso de correo electrónico empresarial.

Este trabajo, se basa en la última red mencionada, VPN, por lo cual se procede a brindar un conocimiento más amplio sobre la misma para el entendimiento del lector.

## Redes privadas virtuales (VPN)

### Introducción a Redes privadas virtuales (VPN)

Para referirse a las VPN, se debe tomar en cuenta las redes LAN o de área local, ya que estas se usan en toda organización; aquí se maneja la comunicación de equipos de la empresa y de sus diferentes áreas. Una compañía, en la actualidad, ya dispone de servicios de Internet para su comunicación con el mundo, tanto para enviar y recibir correos de usuarios externos, como también para consultar diferentes servicios web, sobre todo, bancarios. Adicionalmente, debido al crecimiento, dichas empresas requieren interconectar sus sedes, clientes y también con el personal que se encuentra en un lugar lejano geográficamente.

Para estos usuarios que se encuentran alejados de la empresa, surge la problemática de la comunicación, puesto que requieren un canal seguro para la interconexión con la compañía, donde pueda viajar la información de manera confiable, como si estuviera utilizando su propia red interna.

Utilizar únicamente Internet como medio, genera la posibilidad de que un atacante intercepte la comunicación del usuario con la empresa debido a que la información pasa a través de la red pública.

Una de las primeras soluciones que se plantea, es la utilización de un enlace dedicado, sin embargo, el costo de implementación y renta mensual del servicio que se paga al proveedor de servicios (ISP) es muy elevado y en muchas ocasiones no representa la inversión para una empresa en crecimiento, por ello se opta por el uso del Internet para la transmisión de la información.

Para estos casos, donde el único medio disponible para transmisión es el Internet, se utilizan las Redes VPN. Estas, permiten la creación de una red LAN virtual que permite la conexión de redes físicas a través de un túnel de datos, utilizando protocolos de encriptación para asegurar que la información no sea vulnerable al ser enviada y recibida por un medio poco seguro como lo es la red pública.

Una VPN (red privada virtual), permite acceder de manera confiable a una red LAN (red de área local) sobre una red no regulada como Internet o redes abiertas en general. Permite la transmisión de información estableciendo un túnel de datos peer-to-peer, utilizando para este fin, enlaces dedicados, conexiones encriptadas, o la fusión de los métodos de conexión antes mencionados.

Sobre la interrogante de qué es una VPN, según Eric Crist & Jan Keijser esta definición se resume en que, una red privada virtual permite al administrador de red crear una red 'local' entre varios equipos que se pueden encontrar en distintos segmentos de Red. (Crist & Keijser, 2015).

**Ventajas**

- Protegen y aseguran la confidencialidad de la información, ya que la información viaja encriptada desde el origen hacia el destino.
- Al utilizar encriptación, se garantiza la integridad de la información, puesto que no se puede adulterar la misma al ser enviada o recibida.
- Manejan políticas de autorización y autentificación ya que solo los equipos autorizados pueden acceder a ella desde el punto donde se encuentren, otro dispositivo no accederá a esta red.

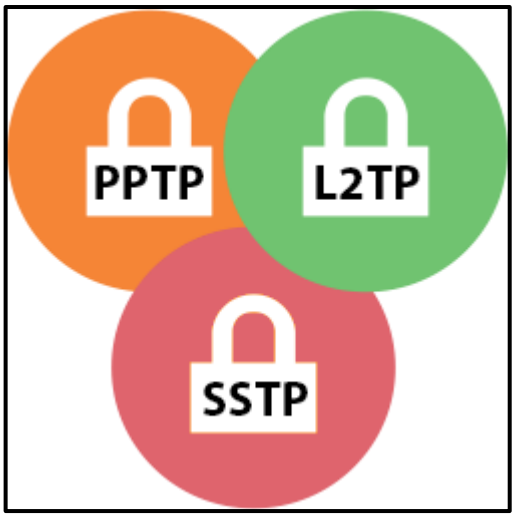
- Los algoritmos utilizados para la compresión de información, facilitan su transferencia.
- En caso de crecimiento de usuarios, no tiene problemas en el escalamiento, se puede acoplar fácilmente para abarcar diferentes localidades.
- Costos reducidos, ya que utiliza el internet como medio de conexión e inversión baja en hardware.
- Fácil de usar; una vez implementada, la conexión a esta red es en muchos casos, casi imperceptible

**Desventajas**

- Deben configurarse adecuadamente las políticas y procedimientos, tanto de acceso como de seguridad.
- Demanda mayor energía y carga, ya que el cliente VPN encapsula la información, para luego cifrarla, esto afecta la batería de dispositivos móviles y en ciertos casos lentitud en la velocidad de transmisión.
- En caso de no existir acceso a Internet, no podremos conectarnos a nuestra VPN.
- La VPN garantiza la seguridad, sin embargo, al viajar por la red pública, sigo estando expuesta a atacantes con mayor experiencia.

**Tipos de protocolos VPN**

**GRÁFICO 3. TIPOS DE PROTOCOLOS VPN**




**Fuente:** http://www.vozidea.com/tipos-protocolos-vpn/

**Elaboración:** Edwin Sánchez

Para la utilización de la tecnología VPN se emplean varios protocolos o tipos de VPN, los cuales pueden ser usados de manera combinada para robustecer la comunicación entre el origen y el destino; los mismos se detallan los mismos a continuación:

- **VPN basada en protocolo PPTP**
- **VPN basada en protocolo IPsec**
- **VPN basada en SSL**
- **OpenVPN**

**Protocolo PPTP**

**GRÁFICO 4. LOGO PPTP**


**Fuente:** http://www.lifewithtech.net/blog/linux/vpn-pptp-server-installation-and-config

**Elaboración**: Edwin Sánchez Estrada

Este protocolo conocido como Point-to-point Tunneling Protocol, fue desarrollado en el año 1999, por las empresas Microsoft, 3Com/Primary Access, Ascend Communications, entre otras, las cuales permitieron la creación de Redes VPN. Esta tecnología es una extensión de PPP (protocolo punto a punto).

Su funcionamiento se basa en encapsular los paquetes PPP mediante un túnel GRE; utiliza el puerto 1723 en TCP por defecto. El cliente PPTP se ha incluido en Windows, desde 1995, y todavía se presenta por defecto en la mayoría de sistemas operativos como Linux y Windows, y dispositivos con iOS y Android. En la actualidad, el protocolo PPTP se

considera potencialmente inseguro, ya que la fuerza de la seguridad de la conexión está directamente relacionada con la fuerza del mecanismo de autenticación elegido (por ejemplo, su contraseña).

En conclusión, una contraseña insegura converge en una conexión VPN insegura. La mayoría de las configuraciones PPTP utilizan el protocolo MS-CHAPv2 para cifrar contraseñas, y es este último el que presenta fallas en su robustez. Su implementación se utiliza para redes donde la fiabilidad no sea requerida ya que una de sus mayores ventajas son las altas tasas de transmisión que ofrece. (Crist & Keijser, 2015, p. 6)

**Protocolo IPsec**

**GRÁFICO 5. LOGO IPSEC**


**Fuente:** http://www.unixwiz.net/techtips/iguide-ipsec.html

**Elaboración**: Edwin Sánchez Estrada

El estándar IPsec es el estándar oficial IEEE/IETF para seguridad IP. IPsec o Internet Protocol security, es un protocolo que trabaja en las capas 2 y 3 del modelo OSI. IPsec añade el concepto de políticas de

seguridad, lo que lo convierte en un protocolo extremadamente potente y flexible, pero complejo al momento de configurar y proceder a solucionar problemas. Fue proyectado para brindar seguridad en la capa de transporte del tráfico de paquetes.

Las políticas de seguridad permiten al administrador de la red cifrar el tráfico entre dos puntos finales en función de varios parámetros, como la dirección fuente y destino, también por los puertos TCP o UDP, emisor o receptor. (Crist & Keijser, 2015, p. 6)

Existen dos maneras de operar en IPsec, el modo túnel y el modo transporte; este último es el más utilizado de manera combinada con el protocolo de túnel de nivel 2 o L2TP. Los clientes IPsec se encuentran por defecto en la mayoría de sistemas operativos, donde se realizar el uso de IPsec + L2TP, sin embargo, también se lo puede utilizar sólo. IPsec permite la configuración para el uso de claves pre-compartidas (pre-shared keys) o certificados X.509 que permiten blindar la conexión VPN. También utiliza contraseñas de una sola vez o protocolos de nombre de usuario/contraseña para autentificar las comunicaciones VPN.

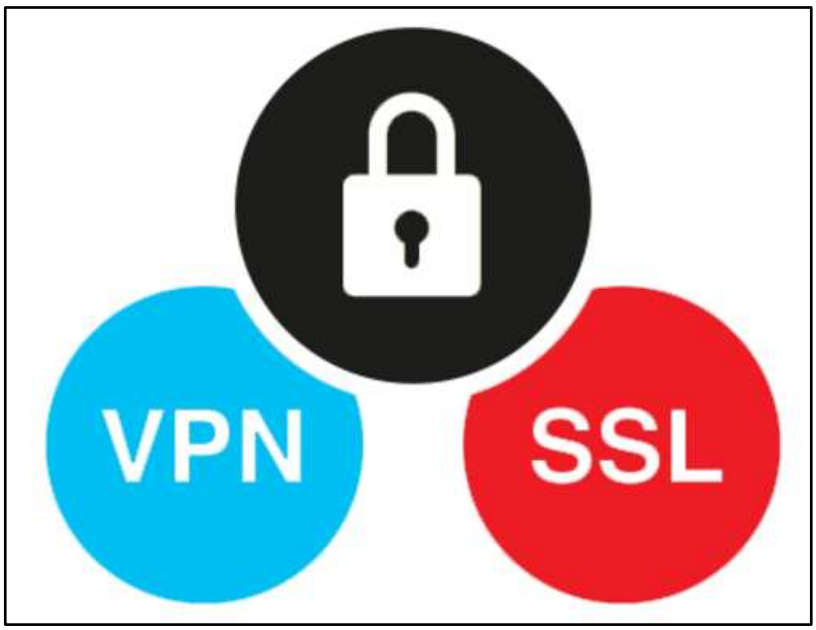
IPsec utiliza dos canales; uno que sirve de control donde controla la configuración para la conexión, y el segundo para el transporte de datos.

El canal de control se establece mediante los puertos UDP 500 o 4500 por defecto, y el canal de datos, emplea el protocolo ESP (IP 50).

La principal desventaja de este protocolo, es que varios proveedores han implementado modificaciones al estándar, lo que dificulta severamente conectar dos puntos IPsec de proveedores diferentes. Cabe recalcar que IPsec viene incluido en la mayoría de sistemas operativos, firewall, enrutadores y concentradores. (Crist & Keijser, 2015, p. 7)

**Protocolo VPN basada en SSL**

**GRÁFICO 6. LOGO SSL**




**Fuente:** http://start-vpn.com/blog-espana/wp-content/uploads/2013/04/openvpn-small.jpg

**Elaboración**: Edwin Sánchez Estrada

SSL, es el tipo de VPN más utilizada hoy en día, se basan en el protocolo SSL/TLS. Las redes privadas virtuales, basadas en SSL son denominadas por lo general 'VPN sin cliente'. Existen ciertos proveedores como Cisco y Microsoft que tienen sus propios clientes para este tipo de conexión. Estas VPN con SSL utilizan el protocolo HTTPS (sitios web seguros).

No existe un estándar completamente definido para las conexiones establecidas mediante SSL, pero en su mayoría se la complementa con TLS para configuración y aseguramiento de estas. La conexión se protege en la mayor parte de los casos utilizando los certificados X.509, contraseñas de una sola vez o protocolos de autenticación empleando usuario y clave. Se utiliza para este fin el protocolo HTTPS sobre el puerto 443 por defecto; sin embargo, existen proveedores que usan complementos en el navegador para 'mejorar' la VPN, pero esto la convierte en no interoperable con sistemas operativos o navegadores no compatibles. (Crist & Keijser, 2015, p. 7)

**Protocolo OpenVPN**

**GRÁFICO 7. LOGO OPENVPN**


**Fuente:** http://start-vpn.com/blog-espana/wp-content/uploads/2013/04/openvpn-small.jpg

**Elaboración**: Edwin Sánchez Estrada

OpenVPN es también llamada VPN basada en SSL; utiliza el protocolo SSL/TLS para blindar la conexión establecida, sin embargo, existe otro protocolo utilizado el cual es HMAC que se combina con un algoritmo adicional para asegurar la integridad de los paquetes transmitidos. Se configura con pre-shared keys como también con certificados X.509, lo cual no se ofrecen en otras VPN basadas en SSL.

Este protocolo utiliza un adaptador de red virtual, denominados TUN o TAP, que sirve como interfaz entre el software instalado y el sistema operativo; por ello, cualquier sistema operativo que tenga soporte y compatibilidad con dispositivos TUN o TAP, puede utilizar el protocolo

OpenVPN. Para su uso, se debe instalar previamente el cliente en el host, esto lo diferencia de las VPN sin cliente o las basadas en web. (Crist & Keijser, 2015, p. 8)

**CUADRO 3. COMPARATIVO ENTRE PROTOCOLOS VPN**

| Comparativo | PPTP | L2TP/IPsec | OpenVPN |
|---|---|---|---|
| Encriptación VPN | 128-bits | 256-bits | 160-bits<br>256-bits |
| Seguridad VPN | Encriptación básica | Encriptación más alta<br>Comprueba la integridad de los datos y los encapsula dos veces. | Encriptación más alta<br>Autentica los datos con certificados digitales. |
| Velocidad VPN | Rápido, debido a un cifrado más bajo. | Requiere más procesamiento de la CPU para encapsular datos dos veces | El mejor protocolo en cuestión de rendimiento. Velocidades rápidas, incluso en conexiones con alta latencia ya través de grandes distancias. |

**Elaboración:** Edwin Eduardo Sánchez Estrada
**Fuente:** Datos de la Investigación

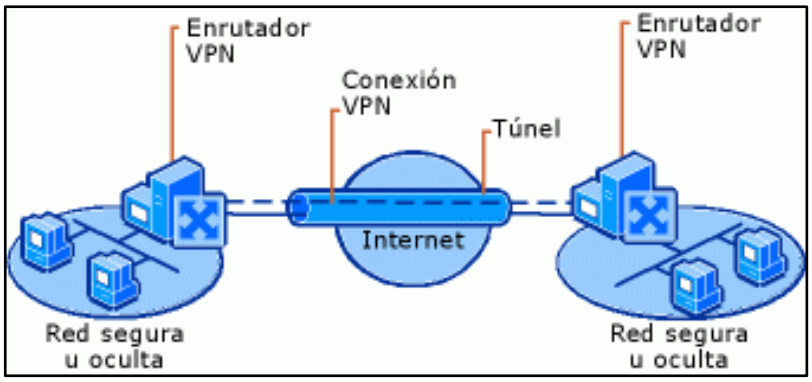
**Tipos de conexiones VPN**

Las VPN disponen de tres arquitecturas para su conexión:

- VPN sitio a sitio
- VPN de acceso remoto
- Tunneling

**VPN sitio a sitio**

**GRÁFICO 8. DIAGRAMA VPN SITIO A SITIO**




**Fuente:** http://elblogdelcommerce.blogspot.es/tags/redes-vpn-tics/

**Elaboración**: Edwin Sánchez Estrada

Interconectan entre sí a redes enteras, un ejemplo de ello es la conexión de una sucursal o agencia, con la sede matriz de una empresa. Cada sitio debe posee un Gateway VPN, el cual puede ser un ruteador, cortafuegos o Switch VPN.

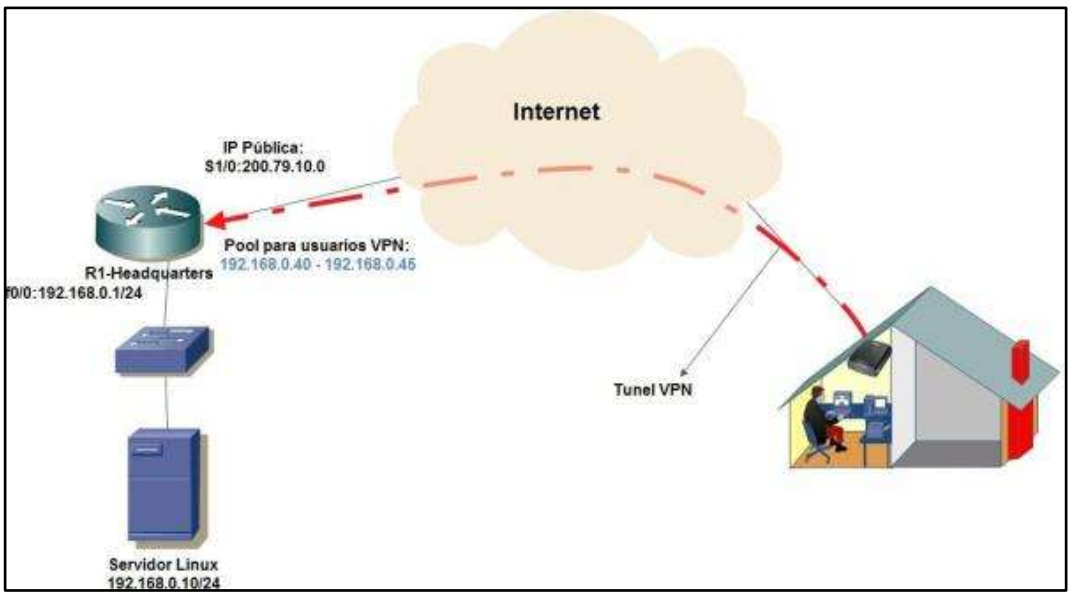
Para establecer la comunicación, los dispositivos deben conocer la configuración VPN con antelación. La conexión VPN permanece estática y los equipos en la red desconocen la existencia de dicha VPN. En este tipo de VPN (site-to-site), se envía el tráfico de datos mediante una pasarela VPN. Esta pasarela es quien realiza las labores de encapsulamiento y cifrado de datos salientes desde un sitio; luego dicha pasarela lo transmite mediante un túnel VPN utilizando Internet hacia la puerta de enlace del destino. Cuando el destino recibe, la puerta de

enlace destino elimina los encabezados, interpreta el contenido y luego realiza el envío del paquete al host destino dentro de su red LAN.

Antes, para realizar estas conexiones entre agencias (redes enteras), se requería utilizar Frame Relay, pero en la actualidad, las empresas se encuentran conectadas a Internet, se pueden ejecutar sin problemas las VPN site-to-site.

**VPN de acceso remoto**

**GRÁFICO 9. DIAGRAMA VPN ACCESO REMOTO**



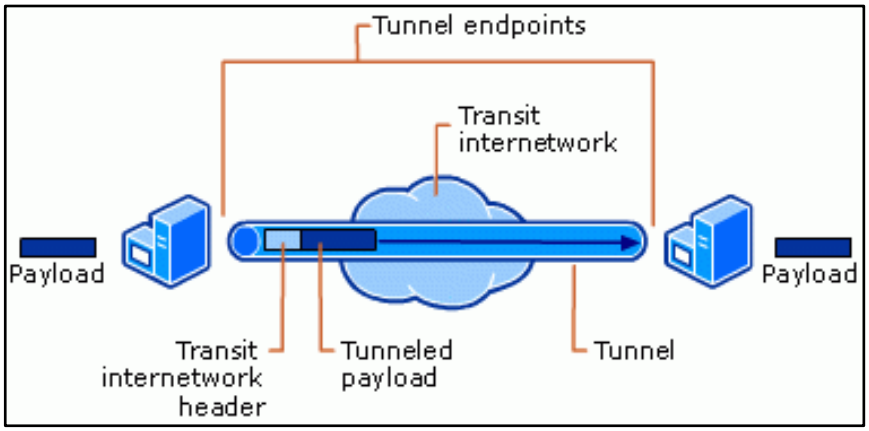

**Fuente:** http://elblogdelcommerce.blogspot.es/tags/redes-vpn-tics/

**Elaboración**: Edwin Sánchez Estrada

Permiten la conexión de dispositivos individuales, hacia la red de una empresa de forma confiable y segura utilizando como medio de enlace el Internet. Frecuentemente para el uso de este esquema el host tiene instalado un cliente VPN basado en Web que permite establecer la conexión VPN.

**Tunneling**

**GRÁFICO 10. DIAGRAMA VPN TUNNELING**




**Fuente:** http://elblogdelcommerce.blogspot.es/tags/redes-vpn-tics/

**Elaboración**: Edwin Sánchez Estrada

Tunneling es una técnica que funciona como protocolo de red encapsulador, realiza la creación de un túnel dentro de una red. Este túnel se establece incluyendo una PDU sobre otra, pudiendo de estar manera transmitirla de extremo a extremo sin que exista la necesidad de interpretar la PDU que viaja encapsulada. De esta manera, los paquetes

de datos se enrutan sobre nodos intermedios que no pueden visualizar claramente su contenido.

**Beneficios de una red VPN**

Una VPN tiene similitud en forma y mantiene ciertas ventajas brindadas por los enlaces dedicados, pero su diferencia radica en la utilización de una red pública utilizando una técnica conocida como tunneling, la cual le permite enrutar los paquetes de datos mediante el Internet, estableciendo un canal privado, emulando a un enlace dedicado.

Este comportamiento permite que en la misma red puedan generarse varios enlaces que pasan a través de diferentes canales virtuales mediante la misma infraestructura.

**Requerimientos básicos de una VPN**

Una red privada virtual requiere las siguientes características para poder ser implementada, y para que la misma funcione de la manera deseada:

**Autenticación de usuario. –** Siempre la VPN deberá tener la posibilidad de identificar que el usuario que está intentando acceder sea el autorizado, caso contrario deberá restringir su acceso. También deben existir registros que permitan generar una auditoria para corroborar que

únicamente los usuarios autorizados hayan accedido (Pazmiño, 2013, p. 44).

**Administración de dirección. –** Dicha VPN debe permitir la asignación de una IP fija al cliente, según el dispositivo autorizado, previamente registrado, del cual se esté conectando.

**Encriptación de información. –** Debido a que los datos van a viajar por una red pública insegura, como lo es el Internet, los datos deben ser inteligibles para los usuarios no autorizados que deseen acceder a ella.

**Administración de llaves. –** Una de las características importantes que debe cumplir una red VPN es la de tener la posibilidad de manejar protocolos comunes, tales como: IP, IPX, etc. Para ello se pueden utilizar protocolos VPN como el PPTP o L2TP, antes mencionados. (Pazmiño, 2013, p. 45)

**Seguridad en VPN**

Las VPN basan el aseguramiento de la información sobre el protocolo que se esté utilizando; sin embargo, dichos estándares emplean ciertos métodos criptográficos para establecer conexión y transmitir datos en el túnel, a dichas metodologías, se las denomina cifrado de información.

**Cifrado de la información**

El cifrado de información conocido como Criptografía es un campo de la criptología que se encarga de utilizar las técnicas para codificar los mensajes haciéndolos solo entendibles para el emisor y receptor autorizado; de esta manera se intenta dar robustez a la confidencialidad de los datos enviados, generando un grado de seguridad adicional a la transmisión de paquetes de datos.

La mayoría de estos sistemas se basan en complejos algoritmos matemáticos que se desarrollan y rediseñan en base a las necesidades que puedan surgir, ya que con el pasar del tiempo estos se vuelven obsoletos o son vulnerados por personas con mayor conocimiento técnico o por intrusos maliciosos que puedan interceptar los mensajes e intenten descifrarlos para hacer daño a una empresa u organización.

La criptología utiliza protocolos criptográficos para la codificación de la información, sobre este tema Escobar (2015), afirma que:

Algunos de estos protocolos son:

- **Protocolos de Autentificación:** el concepto de autentificación puede aludir al mensaje tratando de garantizar que éste no ha sido alterado (autentificación de mensaje) o a la identidad del remitente (autentificación de usuario). La identificación del usuario puede ser directa, comprobando una característica propia de aquel, como la

firma digital o, por el contrario, indirecta, donde el usuario demuestra estar en posesión de una pieza secreta de información.

- **Protocolos para compartir secretos:** distribuir un cierto secreto entre un conjunto P de participantes de forma que ciertos subconjuntos prefijados de P puedan, uniendo sus participaciones, recuperar dicho secreto.
- **Pruebas de conocimiento cero:** permite a un individuo convencer a otro de que posee una cierta información sin revelarle nada sobre el contenido de la misma.
- **Transacciones electrónicas seguras:** permite realizar de forma electrónicamente segura las operaciones bancarias habituales: firma electrónica de contratos, etc.
- **Elecciones electrónicas:** permite realizar un proceso electoral electrónicamente, garantizando la deseable privacidad de cada votante y la imposibilidad de fraude. (Escobar, 2015, p. 29)

**Tipos de cifrado**

Existen varios tipos de cifrados en la actualidad, los mismos se clasifican en 3 grupos:

**Según sus claves:** estos pueden ser simétricos o asimétricos

**Según sus algoritmos:** se dividen en, Cifrado en flujo y cifrado en bloques

**Según sus propiedades:** se clasifican en: cifrado seguro hacia adelante, cifrado con umbral, cifrado basado en identidad, cifrado negable, cifrado con clave aislada, cifrado maleable

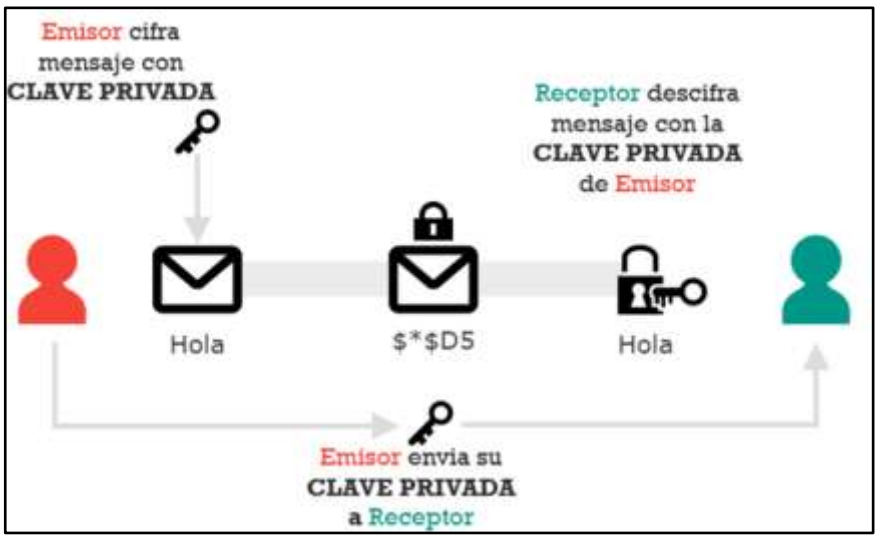
Para la implementación de este trabajo, se utilizarán los cifrados según sus claves, que son los que usan las redes VPN.

Se denominan cifrados simétricos cuando se utiliza la misma clave para encriptar y desencriptar la información

**Definiciones**

**Cifrado simétrico**

**GRÁFICO 11. FUNCIONAMIENTO CIFRADO SIMÉTRICO**




**Fuente:** https://enekoamieva.com/wp-content/uploads/2015/12/cifrado-simetrico.png

**Elaboración**: Edwin Sánchez Estrada

También conocida como cifrado de clave secreta, es una metodología de la criptografía que se basa en la utilización de la misma clave, tanto para codificar como para decodificar la información; por este motivo, siempre el remitente y el destinatario deben estar de acuerdo en la clave a utilizar, luego de ello, el emisor podrá enviar el mensaje de manera codificada y el receptor lo decodificará con la misma clave.

**Compartición de clave:** Una de las debilidades de este método de cifrado es la forma en la que se comparte la clave, debido a que, en caso de que, en el envío de la clave, esta sea interceptada y comprometida, dejará vulnerable la información que se transmita.

**Elevada cantidad de llaves:** Por cada emisor y receptor que exista, se generará un clave que será compartida, es decir, a medida que existan más usuarios utilizando este método, existirá un elevado número de llaves a custodiar.

**Omisión de autenticación:** Al mantener una comunicación por llaves compartidas, cualquier persona que disponga de esta llave, podrá acceder a revisar la información, sin la necesidad de que se valide quien es el usuario.

**Diffie-Hellman**

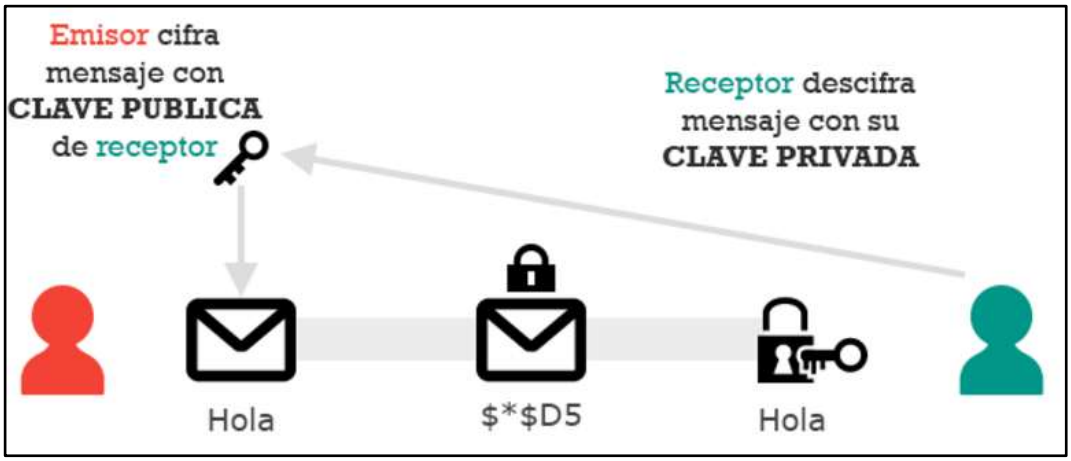
Es un protocolo criptográfico que se utiliza para calcular la longitud de los números primos base que se emplearan durante el intercambio de llaves. Existen 3 grupos que se diferencian por los bits de protección de clave, que son directamente proporcionales a su eficacia:

- Grupo 1: Genera claves de 768 bits
- Grupo 2: Genera claves de 1024 bits
- Grupo 2048: Genera claves de 2048 bits

Los entes negociadores, deben mantener el mismo grupo para que sea posible la interlocución. El fingerprint que resulta de esta negociación, tiene una longitud fija, que no se basa en el tamaño de entrada. Se puede identificar de manera rápida y fácil los errores al momento de la transmisión debido a que su hash MD5 es diferente (Pazmiño, 2013, pág. 43).

**Cifrado asimétrico**

**GRÁFICO 12. FUNCIONAMIENTO CIFRADO ASIMÉTRICO**




**Fuente:** https://enekoamieva.com/wp-content/uploads/2015/12/cifrado-asimetrico.png

**Elaboración**: Edwin Sánchez Estrada

Usualmente identificada como cifrado de clave pública es un sistema criptográfico que se basa en el uso de un par de llaves por entidad para el proceso de codificación y decodificación; de este par de llaves, una es pública y la otra privada, esto quiere decir que, en el caso de la primera, cualquier persona podrá acceder a ella, y la segunda únicamente la tendrá la entidad autorizada para este fin.

Estos algoritmos son diferentes a los simétricos de manera marcada, cuando una clave simétrica es generada, la longitud es escogida de

manera aleatoria, convirtiendo al proceso en complejo. Estos toman el nombre de asimétricos debido a que, en lugar de utilizar una sola clave al codificar y decodificar, utilizan dos; una para descifrar y otra para cifrar; mediante un algoritmo matemático, no se permite que la clave que codifica pueda decodificar y viceversa.

Una clave de cifrado asimétrica se la considera como clave pública, y, la clave de descifrado, se la denomina privada. Como su nombre lo indica, la primera puede ser conocida por todos, pero la privada debe ser ocultada con las precauciones debidas para evitar su vulneración.

**OpenVPN**

Es una solución basada en Open Source (software libre) SSL; fue creado por James Yonan en el 2001, convirtiéndose en un producto multiplataforma, y según Hertzog & Mas, OpenVPN es un software dedicado a crear redes privadas virtuales. Su configuración involucra crear interfaces de red virtuales en el servidor VPN y en los clientes; es compatible con interfaces tun (para túneles a nivel de IP) y tap (para túneles a nivel Ethernet). En la práctica, usualmente utilizará interfaces tun excepto cuando los clientes VPN deban integrar sea la red local del servidor a través de un puente Ethernet. (Hertzog & Mas, 2015, p. 238)

**Ventajas**

- **Únicamente se debe abrir un puerto en el Firewall para admitir las conexiones entrantes:** Desde OpenVPN 2.0, el modo de servidor especial permite múltiples conexiones entrantes en el mismo puerto TCP o UDP, mientras sigue utilizando diferentes configuraciones para cada conexión.
- **Las interfaces virtuales permiten crear reglas redes y firewall específicas:** Todas las reglas, mecanismos de reenvío, restricciones y conceptos, como NAT, se pueden utilizar con los túneles OpenVPN.
- **Alta flexibilidad con opción a utilizar secuencias de comandos:** OpenVPN ofrece numerosos puntos durante la configuración de la conexión para iniciar secuencias de comandos individuales (scripts). Estos scripts se pueden emplear para una gran variedad de propósitos, desde la autenticación hasta la conmutación por error (failover) y más.
- **Soporte transparente y de alto rendimiento para IP dinámicas:** Al utilizar OpenVPN, ya no es existe la necesidad de utilizar IP estáticas en cada lado del túnel. Ambos extremos pueden tener acceso DSL de bajo costo con IP dinámicas y los usuarios rara vez notarán un cambio de IP en ambos lados. Tanto las sesiones de escritorio remoto, como las conexiones SSH parecen bloquearse

durante algunos segundos, pero no finalizarán y continuarán con la acción solicitada después de una breve pausa.

- **NAT sin problemas:** Tanto el servidor OpenVPN como los clientes pueden estar dentro de una red utilizando sólo direcciones IP privadas. Cada firewall puede utilizarse para enviar el tráfico desde un extremo a otro del túnel.
- **Instalación simple sobre cualquier sistema operativo:** Tanto la implementación como el uso, son muy simples; en especial si ya se ha intentado antes configurar conexiones IPsec.
- **Diseño modular:** El diseño modular mantiene un alto grado de simplicidad, tanto en confidencialidad como en red pudiendo ofrecer mejores posibilidades en el mismo rango de seguridad.

**Desventajas**

- **Instalación de cliente:** OpenVPN depende de la instalación de un cliente VPN para poder conectarse con el servidor.
- **Problemas en controlador TAP:** En el sistema operativo Windows se presentan nuevos problemas a medida que van apareciendo nuevas versiones de este S.O.
- **Omisión de interfaz gráfica:** Actualmente no existe una interfaz gráfica para instalación, implementación o gestión de esta herramienta.

- **Incompatibilidad con IPsec:** IPsec es actualmente el estándar VPN, sin embargo, OpenVPN no es compatible con dicha tecnología.
- **Falta de socialización:** En la actualidad aún no hay muchas personas que conozcan el uso de OpenVPN.

**Raspberry PI**

La Raspberry Pi es una computadora pequeña en forma de placa (SBC) que utiliza la arquitectura ARM. Sus inicios datan en el año 2011, en Inglaterra. Creado como proyecto en la Universidad de Cambridge por la Fundación Raspberry PI; su comercialización de manera global empezó en el año 2012.

**Modelos de placas Raspberry PI**

La Raspberry Pi ha evolucionado desde su aparición en 2011, siendo esta frecuentemente utilizada para trabajos académicos por sus características, su integración con otros elementos como Arduino y sobre todo por su costo económico; asimismo, se han creado varios modelos que varían desde su tamaño hasta su funcionalidad. Fue concebida también para la estimulación temprana para la enseñanza de programación, por ello se diseña y comercializa como ordenador de costo económico (Gonzalez & Gainza, 2016). Actualmente existen cinco modelos principales de placas: Raspberry Pi Model A+, Raspberry Pi

Model B+, Raspberry Pi 2, Raspberry Pi 3 y Raspberry Pi Zero. (Upton & Halfacree, 2016).

Para esta implementación se utilizará la placa Raspberry Pi 3, el cual es el último modelo lanzado por la Fundación Raspberry, permite la conexión de dispositivos periféricos mediante sus puertos USB y cableada vía puerto Ethernet incorporado (Perez, 2015). El mismo se basa en sus predecesores, pero integra un nuevo procesador, el Broadcom BCM2837. Este procesador tiene arquitectura de 64 bits y es significativamente más rápido que el BCM2836 utilizado por la Raspberry Pi 2 (Ivković & Radulović, 2016). También se adiciona la posibilidad de conexión inalámbrica a redes Wifi de 2.4GHz, como también permite la interconexión con dispositivos Bluetooth.

Esta tarjeta, al ser pequeña y compacta presenta ciertas limitaciones, sobre este tema Kula asegura que se debe considerar en cada implementación que los cálculos teóricos de uso y que el rendimiento real puede variar ya que por lo general, es más lento que la estimación teórica adaptada en libros (Kula, 2014).

**Raspberry Pi 3**

Su incursión en el mercado fue en febrero de 2016, cambiando su procesador de 900 MHz a 1.2GHz, dentro de las mejoras significativas

realizadas, se encuentra la incorporación de conexión bluetooth 4.1 BLE (Bluetooth Low Energy) y de la tecnología Wifi 802.11n permitiendo las comunicaciones inalámbricas.

**Especificaciones técnicas**

La placa Pi 3, cuenta con las siguientes especificaciones técnicas:

- Procesador ARMv8 CPU 1.2GHz 64-bit de 4 núcleos
- 802.11n Wireless LAN
- Bluetooth 4.1
- Bluetooth Low Energy (BLE)
- 1GB de memoria RAM
- 4 puertos USB
- 40 pines GPIO
- Puerto Full HDMI
- Puerto Ethernet
- Conector de audio combinado de 3.5mm y video compuesto
- Interfaz para cámara (CSI)
- Interfaz para display (DSI)
- Ranura para tarjeta Micro SD
- Núcleo para gráficos VideoCore IV 3D

**Ventajas**

- Bajo consumo de energía frente a un PC convencional.
- Bajo costo de adquisición frente a otros equipos con las mismas prestaciones.
- Comunidad de usuarios en crecimiento constante.
- Desarrollo amplio y variado de proyectos que implementan su uso.
- Su tamaño compacto, el cual permite su fácil traslado.
- Su capacidad de procesamiento es alta, en relación a otros dispositivos del mismo tamaño y costo.

**Desventajas**

- Requiere de conocimientos técnicos para su uso e implementación
- Su capacidad de procesamiento no está optimizada para trabajar con particiones NTFS utilizadas por Windows.
- No soporta la alimentación de discos duros portátiles u otros dispositivos que demanden mayor cantidad de energía.
- Para la utilización de sus dos puertos USB y el puerto de conexión Ethernet, comparten el mismo bus, lo cual limita la velocidad de transferencia.

## Arquitectura ARM

ARM, acrónimo de la firma inglesa Advanced Risc Machines, quién utiliza la arquitectura RISC (Ordenador con Conjunto Reducido de Instrucciones, en su traducción al español), es una arquitectura creada originalmente por Acorn, para el uso de computadores personales, su primera aparición comercial se dio en 1987.

Esta arquitectura nació para la utilización de dispositivos y computadores de bolsillo; en la actualidad los podemos encontrar en celulares, tabletas, ruteadores, televisores, lavadoras, etc., se posiciona como una solución por su bajo consumo de energía eléctrica y por su costo económico al momento de la fabricación de chips. Esta tecnología se encuentra en crecimiento y se le avecina un futuro muy prometedor en esta sociedad que intenta abaratar costos mientras se es responsable con el medio ambiente.

## Dispositivos con Arquitectura ARM

En la actualidad, existe una gran variedad de dispositivas que manejan esta arquitectura, entre ellos se encuentran los smartphones, por ejemplo.

**ARM vs. x86**

Los dispositivos x86 son los más utilizados en equipos personales, sean Desktop o laptops. Su arquitectura es basada en CISC (Complex Instruction Set Computing)

En su lugar los dispositivos que utilizan procesador ARM son basados en la arquitectura Reduced Instruction Set Computer (RISC, por sus siglas en ingles).

Aquí podremos detallar algunas diferencias claves de estos tipos de procesadores:

**x86:**

- Intel es el único fabricante y diseñador de procesadores x86.
- Brinda mayor énfasis a la velocidad y el rendimiento que al consumo de energía eléctrica.
- Es compatible con la mayoría de sistemas operativos, incluyendo Linux, Windows, Android; y ellos consumen mucha energía.
- Es un procesador utilizado por computadores de escritorio, portátiles y servidores.

**ARM:**

- Se enfoca principalmente en el bajo consumo de energía eléctrica.
- Soporta los sistemas operativos Android y Linux.
- Estos procesadores son utilizados en dispositivos como Smartphones, Tablets, Phablets, iPads, Raspberry, etc.

**Qué es Latch**

Es un servicio creado y provisto por Eleven Paths, una filial de Telefónica S.A., que permite proteger el acceso a cuentas digitales como Facebook, Twitter, etc. La idea básica es la de limitar el acceso y el tiempo de exposición a dichas cuentas digitales, ante un posible acceso no autorizado; donde únicamente será el propio usuario el que decide si sus cuentas estarán bloqueadas o desbloqueadas a la hora de requerir acceder a ellas. (Telefónica Digital Identity, 2015b, p. 3)

Latch permite agregar una capa adicional, puesto que no reemplazará el ingreso de credenciales (usuario y contraseña), por el contrario, mantendrá un 'pestillo' que deberá activar el usuario antes de ingresar a la aplicación deseada, de esta manera, aunque alguien obtenga de manera fraudulenta sus datos de inicio de sesión, no podrá acceder sin la previa autorización de este servicio.

**Requisitos para utilización de Latch**

El servicio Latch, presenta los siguientes requisitos para su uso:

- Poseer un dispositivo móvil Smartphone donde debe existir la aplicación Latch instalada.
- Poseer una cuenta digital en las plataformas que son soportadas por el servicio Latch (Tuenti, Facebook, Twitter, entre otras). (Telefónica Digital Identity, 2015a, p. 3)

## FUNDAMENTACIÓN SOCIAL

El proyecto beneficiará la productividad de la empresa, pero cabe recalcar que los colaboradores que se conectarán remotamente viajan constantemente para que lugares lejanos y remotos, que tengan acceso a internet, puedan tener la posibilidad de recaudar diferentes servicios, como agua, luz, teléfono, internet, recargas, pagos de pensiones alimenticias, RISE, entre otros, para evitar que el usuario final tenga que viajar mes a mes para cancelar sus obligaciones pendientes.

## FUNDAMENTACIÓN LEGAL

Sobre la utilización de Software Libre, se mencionan los siguientes artículos que se detallan en el Decreto 1014, de 10 de abril de 2008, incluido en el segundo suplemento N. 714 del Registro Oficial.

**Artículo 1.-** Establecer como política pública para las Entidades de la Administración Pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos.

**Artículo 2.-** Se entiende por Software Libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Estos programas de computación tienen las siguientes libertades:

a) Utilización del programa con cualquier propósito de uso común.

b) Distribución de copias sin restricción alguna.
c) Estudio y modificación del programa (Requisito: código fuente disponible).
d) Publicación del programa mejorado (Requisito: código fuente disponible).

**Artículo 3.-** Las entidades de la Administración Pública Central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software.

**Articulo 4.-** Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de Software libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

Para efectos de este derecho se comprende como seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa del patrimonio nacional.

Sobre la seguridad de los servicios de telecomunicaciones brindados, establecido en la Ley Orgánica de Telecomunicaciones publicada en el Registro Oficial N. 439, el 18 de febrero del 2015; el abonado estará obligado a:

**Artículo 23.-** Obligaciones de los abonados, clientes y usuarios.

**2.-** Adoptar las medidas sugeridas por el prestador de servicios a fin de salvaguardar la integridad de la red y las comunicaciones, sin perjuicio de las responsabilidades de los prestadores.

Sobre los delitos contra el derecho a la propiedad, según lo establecido en el Código Orgánico Integral Penal, publicado en el Registro Oficial N. 180, el 10 de febrero del 2014, se detalla el siguiente artículo:

**Artículo 190.- Apropiación fraudulenta por medios electrónicos.** - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada

con pena privativa de libertad de uno a tres años.

## Hipótesis

Con la implementación de la red VPN se logrará interconectar a los usuarios remotos que requieren acceder a la red corporativa, asegurando la conectividad, seguridad, disponibilidad y accesibilidad a la red. Se brindarán los mecanismos necesarios para que los usuarios puedan

gestionar los requerimientos concernientes a la empresa, sin dejar de lado la integridad de la información, evitando generar acumulación de trabajo, falta de seguimiento a novedades o problemáticas que puedan surgir en la compañía, mejorando la productividad de los colaboradores de la empresa Reporne S.A. que se encuentren geográficamente alejados.

## Variables de la investigación

### Variable Independiente

Para esta implementación, las variables independientes son todas las que pueden afectar directamente la implementación o la operatividad de la red y del equipo, tales como:

- Ancho de banda disponible para la ejecución de esta implementación.
- Permisos para el acceso a la red interna (limitación a equipos según las políticas de la compañía).
- Climatización deficiente o nula en el lugar que la empresa designe para la instalación del equipo.
- Problemas en la instalación eléctrica donde se instale el equipo.
- Seguridad física en la ubicación del dispositivo

.

**Variable Dependiente**

- Uso indiscriminado del ancho de banda el cual disminuirá el desempeño de la red VPN.
- Acceso limitado a ciertos servicios de la empresa que no permita gestionar una actividad urgente
- Avería de equipos por sobrecalentamiento y falta de climatización.
- Daño total del dispositivo por motivos de variación de voltaje o cortes de energía abruptos.
- Manipulación no autorizada del equipo por parte de terceros, de manera accidental o mal intencionada debido a su tamaño.

## DEFINICIONES CONCEPTUALES

**VoIP. –** Es el termino donde se hace referencias a varios recursos que permiten gestionar el viaje de señales de voz a través de una red, mediante el protocolo TCP/IP, convirtiéndolas desde su origen análogo a digital, para su transporte, y luego nuevamente a análogo, para su destino.

**Host. –** Se denomina de esta manera, en informática, a los dispositivos conectados en una red, los cuales utilizan los servicios que esta provee para sus diferentes propósitos.

**Conexión remota. –** es una tecnología que permite conectarse a un dispositivo desde otro, conectado desde cualquier parte del globo, para poder utilizarlo, administrarlo o transferir información entre ellos.

**Peer-to-peer. –** Esta tecnología permite la conexión entre dos puntos únicamente, esto se puede dar con hosts, firewalls, o cualquier equipo de comunicación que mantenga este diseño de enlace.

**ARPANET. –** fue una red creada por el Departamento de Defensa de los Estados Unidos que permitía la comunicación a organismos

gubernamentales de dicho país, en primera instancia. Se considera el inicio del Internet.

**NSFNET. –** desarrollada por la Fundación Nacional para la Ciencia como un proyecto que interconectaba cinco superordenadores permitiendo la ampliación del Internet, puesto que mejoró la infraestructura de telecomunicaciones en el año 1986.

**Wireless. –** Es el término que se emplea para hacer mención redes de comunicaciones inalámbricas, es decir, que no usan cables para su conexión, sino que se realiza mediante ondas electromagnéticas.

**FireWire. –** es un puerto cableado que permite la transmisión de información de manera permanente, sin interrupciones. Es ideal para transmisión de audio y video en tiempo real.

**Bluetooth. –** es una especificación de tecnología inalámbrica que permite realiza la transmisión de información entre dispositivos en un radio de corto alcance.

**USB. –** es el estándar de comunicación más utilizado hoy en día, el cual permite comunicar, conectar y brindar alimentación de energía a los dispositivos que lo utilizan.

**IrDA. –** es una tecnología creada en 1993 la cual permite la transmisión de comunicación de manera inalámbrica, pero solo a una distancia entre 5 a 60 centímetros; fue reemplazada por Bluetooth.

**Repositorio. –** En tecnología, se denomina repositorio a un lugar donde se almacenan archivos, bases de datos o cualquier tipo de información; estos pueden ser de uso restringido o abierto.

**ISP. –** hace referencia a la empresa que provee de servicios de Internet y de comunicaciones, como enlace de datos, hacia una empresa o a clientes masivos.

**Encriptación. –** es un sistema que permite codificar información. Es utilizado en la informática generalmente para la generación de contraseñas y credenciales digitales.

**GRE. –** es un protocolo que brinda la posibilidad de establecer túneles mediante Internet utilizando un esquema de encapsulamiento.

**MS-CHAPv2. –** es una versión del protocolo de autenticación de claves propietaria de Microsoft.

**Modelo OSI. –** es un modelo de referencia donde se muestra una arquitectura en capas el cual fue creado por la Organización Internacional de Normalización.

**TCP. –** es un protocolo que posibilita la transmisión de datos garantizando que los datos lleguen a su destino sin errores y en el mismo orden en el que fueron transmitidos.

**UDP. –** es un protocolo que realiza intercambio de datagramas y que no garantiza que el paquete llegue correctamente ni saber en qué orden fueron recibidos por el destino.

**ESP. –** es un método de encriptación por encapsulamiento que brinda mayor confidencialidad a los datos, integridad y autenticación.

**HMAC. –** es un código criptográfico que se usa para verificar la integridad de los datos y la autenticación del mensaje transmitido.

# CAPÍTULO III

# METODOLOGÍA DE LA INVESTIGACIÓN

## DISEÑO DE LA INVESTIGACIÓN

### Modalidad de la investigación

La modalidad de la investigación que se utilizará en esta implementación se describe como proyecto factible ya que utiliza Software de código abierto dentro de su instalación y ejecución; el cual no genera costos, ni de adquisición de licencias o del programa como tal, generando mayores beneficios en desarrollo de dicho proyecto.

El proyecto se considera factible debido a que aportará con herramientas que permitirán optimizar los tiempos de respuesta y mejorar la calidad de servicio a los clientes finales, impactando positivamente en la productividad e imagen externa hacia los usuarios, sobre esta modalidad.

En base a lo mencionado, un proyecto factible se define como un conjunto de actividades vinculas y que en su ejecución se lograrán los objetivos establecidos en relación a las necesidades que puedan existir en una entidad o grupo social en un momento específico. (Dubs de Moya, 2002).

En este proyecto de investigación se empleará OpenVPN como servidor VPN el cual se complementará con la red de la empresa, también se utilizará la aplicación Latch para brindarle una capa adicional de seguridad a esta implementación con el fin de que el personal que se encuentre fuera de la empresa pueda conectarse desde cualquier punto remoto con acceso a Internet en caso de situaciones emergentes o por temas laborables en condiciones controladas por el administrador de redes.

**Tipos de investigación**

**Por el lugar**

**De campo. –** El proyecto que se desea implementar en la empresa permite la recolección de información de datos reales y fidedignos que se procederán a analizar mediante la observación, y encuestas que se realizarán en el lugar donde se desarrollan los hechos.

**Por la naturaleza**

**Para la toma de decisiones. –** La empresa en la actualidad posee redes VPN que se conectan site-to-site, es decir, de firewall a firewall, lo que le permite la administración de equipos remotos en instalaciones previamente configuradas, sin embargo, no existe una solución que permite conectar a usuarios en modelo cliente/servidor, es decir que el cliente pueda estar en cualquier parte del mundo, previo a la configuración y autorización de su equipo.

**Por la factibilidad**

**Proyecto factible. –** el proyecto, luego de la investigación realizada, se encasilla como factible debido a su rentabilidad económica, poca complejidad de la instalación y su uso intuitivo.

Este proyecto se desarrollará en la empresa Reporne S.A. donde se ha analizado la factibilidad de su implementación y su utilidad para los usuarios que se encuentren fuera de la empresa donde se optimizará la productividad y el tiempo de respuesta ante quejas, reclamos o solicitudes varias.

**Población y muestra**

Debido a al ámbito de seguridad y brindar accesos autorizados, la población será únicamente el personal administrativo de las diferentes áreas de la empresa, las cuales son: Sistemas, Producción, Infraestructura, Financiero, Comercial, Operaciones, OyM y Administración. La muestra será el 100% puesto que el total de personas que trabajan en la empresa, en las áreas antes mencionadas, es de 23 colaboradores. En la encuesta se realizaron 12 preguntas relacionadas a la necesidad de implementar esta mejora y para determinar si tienen conocimiento sobre las VPN.

La distribución de la muestra se realizará bajo el siguiente cuadro:

**CUADRO 4. DISTRIBUCIÓN DE MUESTRA POR DEPARTAMENTO**

| Muestra | Cantidad |
|---|---|
| Operaciones | 5 |
| Sistemas | 4 |
| Producción | 3 |
| Comercial | 3 |
| Administración | 2 |
| Financiero | 2 |
| OyM | 1 |
| Gerencia | 1 |
| Infraestructura | 1 |
| Recursos Humanos | 1 |
| Total | 23 |

**Fuente:** Trabajo de investigación
**Elaboración:** Edwin Sánchez Estrada

## Técnicas e instrumentos de recolección de datos

Para la recolección de datos en este trabajo de investigación, utilizaremos la encuesta, la cual cuenta con 12 preguntas que permitirá conocer la situación actual de la empresa y validar la necesidad de realizar la implementación del proyecto propuesto.

## Recolección de la información

La información será recopilada en la oficina matriz de la empresa Reporne S.A., ubicada en la ciudad de Guayaquil; mediante una encuesta de 12 preguntas realizada el 25 de agosto de 2017, la cual está dirigido a 23 colaboradores que corresponden al personal con cargo administrativo de las diferentes áreas de la empresa.

## Procesamiento y análisis

Para poder determinar el procesamiento y análisis de las encuestas realizadas al personal con cargos administrativos de la empresa Reporne S.A., se utilizará el método de tabulación en una hoja de Excel. Debido a que la población es de 23 personas únicamente, no se aplicarán formulas, pero se encuestará a todo el universo muestral. Luego de tabular las respuestas, se generarán diagramas de pastel para la visualización de los resultados.

**Pregunta 1**

**¿Qué tan frecuente usted se ausenta de la empresa por motivos laborales?**

**CUADRO 5. RESULTADO DE LA ENCUESTA: PREGUNTA 1**

| Opciones | Total | Porcentaje |
|---|---|---|
| Frecuentemente | 6 | 26% |
| Nunca | 3 | 13% |
| Ocasionalmente | 14 | 61% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 13. RESULTADO DE LA ENCUESTA: PREGUNTA 1**


**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** Se observa que el 61% de 23 personas encuestadas, consideran que su ausentismo en la empresa, por temas laborales, lo realiza de manera ocasional; es decir que el proyecto de implementación se ajusta a la necesidad, puesto que permitirá que estos usuarios, que no viajan de manera frecuente, puedan conectarse a la red corporativa sin saturar el rendimiento del equipo.

**Pregunta 2**

**En caso de estar ausente y requerir atender o gestionar un tema urgente de la empresa, ¿Cómo procede?**

**CUADRO 6. RESULTADO DE LA ENCUESTA: PREGUNTA 2**

| Opciones | Total | Porcentaje |
|---|---|---|
| Abandona la actividad que esté realizando, y acude inmediatamente a la empresa. | 2 | 9% |
| Delega el tema a otro colaborador | 14 | 61% |
| El tema debe esperar hasta que usted se encuentre en la empresa. | 7 | 30% |

**Elaborado por:** Edwin Sánchez Estrada
**Fuente:** Datos de la encuesta

**GRÁFICO 14. RESULTADO DE LA ENCUESTA: PREGUNTA 2**


**Elaborado por:** Edwin Sánchez Estrada
**Fuente:** Datos de la encuesta

**Análisis:** De las 23 personas, se puede confirmar que cuando existe ausencia de la persona encuestada, por motivos laborales, el 61% debe delegar el tema surgido a otro colaborador, afectando de manera directa la productividad de la persona que se encuentra en oficina, quien deberá dejar de atender sus requerimientos, por revisar la tarea adicional solicitada.

El 30% opta por esperar a volver a la empresa para gestionar el tema, quedando el caso desatendido, donde quizá implique directamente en una multa económica o en una mala percepción hacia el cliente final. Adicional hay un 9% acude a la empresa de manera urgente, dejando a un lado las actividades que pueda estar ejecutando en ese momento.

**Pregunta 3**

**¿Conoce usted cómo funcionan las Redes Privadas Virtuales o VPN?**

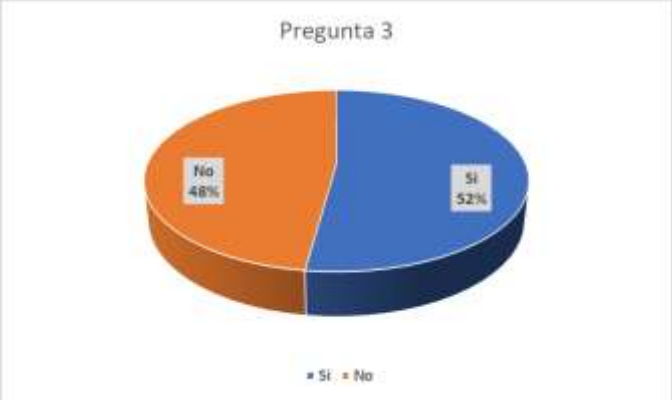
**CUADRO 7. RESULTADO DE LA ENCUESTA: PREGUNTA 3**

| Opciones | Total | Porcentaje |
|---|---|---|
| Si | 12 | 52% |
| No | 11 | 48% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 15. RESULTADO DE LA ENCUESTA: PREGUNTA 3**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** Al consultar a los encuestados sobre el conocimiento de las redes VPN, se obtiene que el 52% asegura conocer su funcionamiento, mientras que el 48% admite desconocer el tema; esto se debe a que los colaboradores no han usado este servicio, sólo realizan el uso dentro de la red LAN de la empresa.

**Pregunta 4**

**¿Considera usted qué es seguro conectarse desde una red abierta o desconocida, hacia el Internet?**

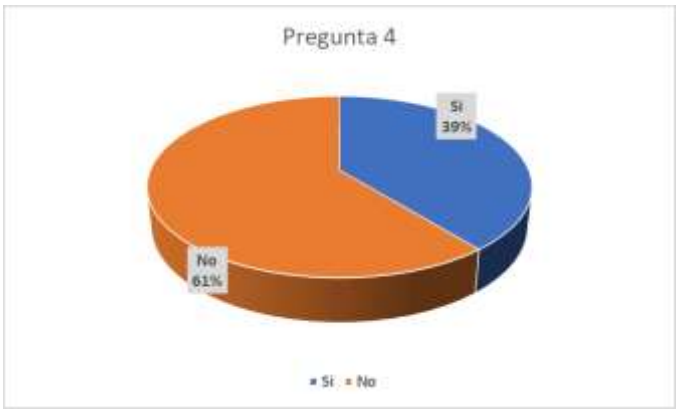
**CUADRO 8. RESULTADO DE LA ENCUESTA: PREGUNTA 4**

| Opciones | Total | Porcentaje |
|---|---|---|
| Si | 9 | 39% |
| No | 14 | 61% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 16. RESULTADO DE LA ENCUESTA: PREGUNTA 4**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** De los 23 colaboradores encuestados, el 39%, considera que, al conectarse a una red abierta o desconocida, está navegando de manera segura en Internet; sin embargo, el 61% tiene presente que estas redes son vulnerables y que la información que viaja, es susceptible a ser interceptada, derivando en el robo de datos, fraudes electrónicos, o suplantación de identidad; por lo cual es necesaria la implementación de una VPN donde la data viaje cifrada y solo el destino pueda interpretarla.

**Pregunta 5**

**¿Cree usted qué es necesario tener un medio de conexión seguro a la empresa, para atención de temas emergentes?**

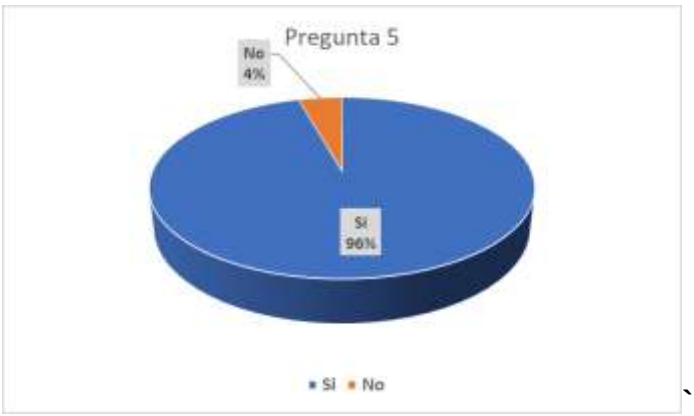
**CUADRO 9. RESULTADO DE LA ENCUESTA: PREGUNTA 5**

| Opciones | Total | Porcentaje |
|---|---|---|
| Si | 22 | 96% |
| No | 1 | 4% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 17. RESULTADO DE LA ENCUESTA: PREGUNTA 5**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** De 23 personas encuestadas, se pudo constatar que el 96% considera necesario un método de conexión seguro hacia la empresa para la atención de temas emergentes; esto debido a que la actividad de la empresa se basa en transacciones en línea donde cada segundo existe entrada y salida de dinero. Es necesario que, en caso de que exista una conexión desde el exterior de la empresa, esta sea segura; por ello se propone el uso de OpenVPN.

**Pregunta 6**

**¿En qué departamento de la empresa usted desempeña sus funciones?**

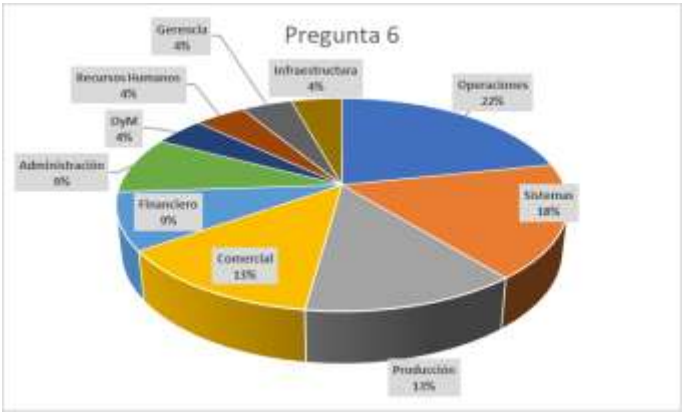
**CUADRO 10. RESULTADO DE LA ENCUESTA: PREGUNTA 6**

| Opciones | Total | Porcentaje |
|---|---|---|
| Operaciones | 5 | 21,7% |
| Sistemas | 4 | 17,4% |
| Producción | 3 | 13,0% |
| Comercial | 3 | 13,0% |
| Financiero | 2 | 8,7% |
| Administración | 2 | 8,7% |
| OyM | 1 | 4,3% |
| RRHH | 1 | 4,3% |
| Gerencia | 1 | 4,3% |
| Infraestructura | 1 | 4,3% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 18. RESULTADO DE LA ENCUESTA: PREGUNTA 6**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** Se consultó a los 23 colaboradores que participaron en la encuesta, el departamento donde desarrollan sus actividades, para saber la necesidad de poseer un método de conexión seguro en las áreas mostradas en el grafico 19.

**Pregunta 7**

**Cuando se encuentra fuera de la oficina, ¿Qué tan probable es encontrar un punto de acceso a Internet?**

**CUADRO 11. RESULTADO DE LA ENCUESTA: PREGUNTA 7**

| Opciones | Total | Porcentaje |
|---|---|---|
| Muy probable | 12 | 52% |
| Poco probable | 11 | 48% |
| Improbable | 0 | 0% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 19. RESULTADO DE LA ENCUESTA: PREGUNTA 7**


**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** Se consultó a los 23 encuestados, sobre la probabilidad que tiene de encontrar un punto de acceso para conectarse a Internet. El 52% calificó que es muy probable; el 48% mencionó que la probabilidad es baja, y ninguno indicó que esta opción sea improbable. Cabe recalcar que la empresa dispone de dispositivos de internet inalámbrico banda ancha (MiFi) mediante la red celular, los cuales pueden ser provistos a los colaboradores en sus viajes para que puedan conectarse en caso de no poder acceder a una red abierta con salida a Internet.

**Pregunta 8**

**¿Considera usted qué es importante implementar métodos de seguridad para evitar el robo de información cuando existan conexiones remotas a la empresa?**

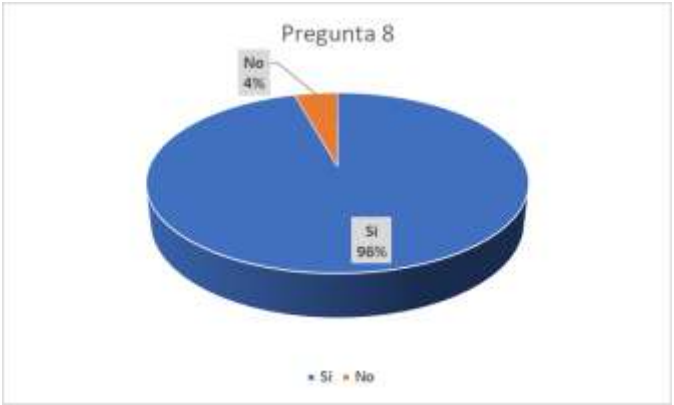
**CUADRO 12. RESULTADO DE LA ENCUESTA: PREGUNTA 8**

| Opciones | Total | Porcentaje |
|---|---|---|
| Si | 22 | 96% |
| No | 1 | 4% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 20. RESULTADO DE LA ENCUESTA: PREGUNTA 8**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** Se observa que el 96% de 23 personas encuestadas, consideran es importante mantener métodos de seguridad cuando se conecten a la empresa, a fin de evitar robo de información; por lo cual la implementación de OpenVPN se ajusta a esta necesidad, y al colocarle una capa adicional de robustez como es Latch, se podrá evitar que los datos y componentes sensibles de la empresa, sean atacados.

**Pregunta 9**

**¿Cómo evalúa usted la posibilidad de que se pueda establecer una conexión remota a la red de la empresa, para revisión de temas laborables emergentes?**

**CUADRO 13. RESULTADO DE LA ENCUESTA: PREGUNTA 9**

| Opciones | Total | Porcentaje |
|---|---|---|
| Excelente | 17 | 74% |
| Buena | 6 | 26% |
| Mala | 0 | 0% |
| Pésima | 0 | 0% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 21. RESULTADO DE LA ENCUESTA: PREGUNTA 9**


**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** De los 23 colaboradores encuestados, el 74% considera que es una excelente opción conectarse de manera remota a la empresa para la atención de temas emergentes; el 26% considera que la idea es buena. Aquí se evidencia la importancia de establecer una vía para comunicación externa, que permita acceder a los recursos de la empresa de manera segura y controlada, esto mediante un túnel VPN.

**Pregunta 10**

**¿Dispone usted de un dispositivo portátil provisto por la empresa, como laptop o Tablet, para uso laboral?**

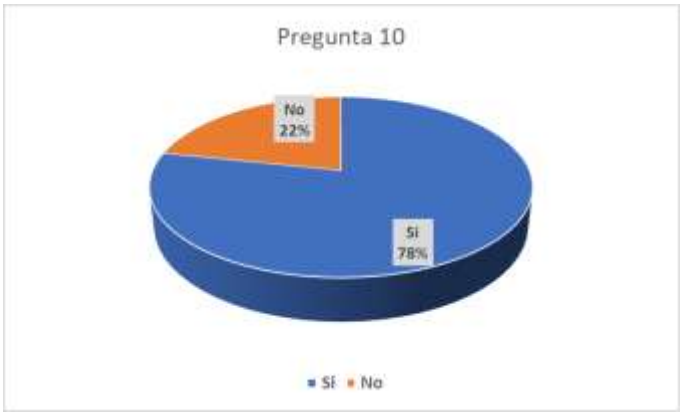
**CUADRO 14. RESULTADO DE LA ENCUESTA: PREGUNTA 10**

| Opciones | Total | Porcentaje |
|---|---|---|
| Si | 18 | 78% |
| No | 5 | 22% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 22. RESULTADO DE LA ENCUESTA: PREGUNTA 10**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** El 78% de la muestra de 23 personas, afirma poseer un dispositivo móvil provisto por la empresa, para uso laboral; permitiendo la instalación del cliente OpenVPN en dichos dispositivos para su posterior configuración y así puedan conectarse de manera remota cuando se encuentren fuera de la empresa, siempre y cuando el administrador de infraestructura los autorice previamente.

**Pregunta 11**

**En caso de encontrarse en una localidad remota y conectarse a la empresa mediante una Red Privada Virtual, ¿Qué aspectos usted preferiría de esta conexión?**

**CUADRO 15. RESULTADO DE LA ENCUESTA: PREGUNTA 11**

| Opciones | Total | Porcentaje |
|---|---|---|
| Todas las anteriores | 13 | 57% |
| Seguridad | 4 | 17% |
| Rapidez | 4 | 17% |
| Confidencialidad | 2 | 9% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 23. RESULTADO DE LA ENCUESTA: PREGUNTA 11**


**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** De los 23 individuos consultados mediante la encuesta, el 57% considera que es importante tener los aspectos de seguridad, rapidez y confidencialidad dentro de una conexión VPN; el 17% considera que es importante solo la rapidez; otro 17% afirma que solo debe ser segura y un 9% que únicamente la confidencialidad debe ser considerada. La red VPN cuenta con estos 3 aspectos que son indispensables para cualquier empresa y que permite encriptar la información y solo sea vista por el otro extremo del túnel de datos.

**Pregunta 12**

**¿Considera usted que la implementación de una Red Privada Virtual segura, que le permita conectarse remotamente, ayudará a mejorar la productividad de la empresa?**

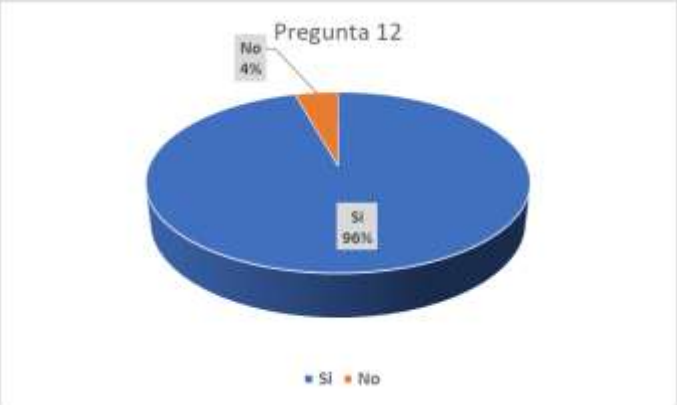
**CUADRO 16. RESULTADO DE LA ENCUESTA: PREGUNTA 12**

| Opciones | Total | Porcentaje |
|---|---|---|
| Si | 22 | 96% |
| No | 1 | 4% |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**GRÁFICO 24. RESULTADO DE LA ENCUESTA: PREGUNTA 12**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos de la encuesta

**Análisis:** El 96% de los 23 colaboradores encuestados, está de acuerdo que existiría una mejora en la productividad al poder conectarse de manera remota, sobre todo en temas emergentes cuando no se encuentra en la oficina; ya que de esta manera se podrá mantener comunicación con la empresa cuando sea requerido, generando mejores tiempos de respuesta y evitar acumular actividades o delegando a otro colaborador, por ello, esta implementación ayudará a la empresa de manera directa.

**Validación Hipótesis**

De acuerdo a la encuesta realizada a los colaboradores de la empresa Reporne S.A., en la ciudad de Guayaquil, sobre la factibilidad de crear una Red Privada Virtual (VPN), se valida la hipótesis debido a que en la actualidad no existe en la compañía una herramienta que permita establecer comunicación hacia la misma, cuando el personal se encuentre fuera de las instalaciones por temas laborales; de esta manera se propone generar, mediante esta implementación, un método seguro y confiable para este fin.

# CAPÍTULO IV

# PROPUESTA TECNOLÓGICA

Luego de realizar la investigación de campo y según los resultados obtenidos, se procede a realizar la propuesta con el fin de mejorar la productividad de los colaboradores de la empresa Reporne S.A. y de agilitar el tiempo de solución en caso de que el responsable de la actividad, se encuentra fuera de la oficina por motivos laborales. La integración de la VPN a la red corporativa, permitirá la conexión de usuarios remotos, previamente autorizado por el departamento de Infraestructura, siempre que tengan un punto de acceso a Internet disponible. Se escoge el servidor OpenVPN debido que permite establecer conexiones seguras mediante una infraestructura pública, utilizando el protocolo SSL y combina la mayoría de características de otras soluciones VPN.

En cuanto al control, se podrá llevar un registro de las conexiones realizadas mediante los registros generados en el servidor OpenVPN y también los intentos de acceso no autorizados que pudiesen existir utilizando el aplicativo Latch. Estos servicios y aplicaciones, serán instalados en una Raspberry Pi, la cual permitirá aprovechar su arquitectura ARM a un costo económico.

## PROPUESTA DEL PROYECTO

### 1. Descripción de la propuesta:

La propuesta realizada a la empresa REPORNE S.A. se basa en la necesidad de trabajar de manera remota para colaboradores específicos de la compañía que, por motivos laborales o personales, se encuentren fuera, dejando desatendidas las tareas asignadas, de manera eventual o recurrente. Actualmente no se cuenta con un método que permita este sistema de teletrabajo, ocasionando desinformación, dilatación de tiempos de respuestas de requerimientos, acumulación de actividades y/o sobrecarga a colaboradores

### 2. Planeación del proyecto:

El objetivo del proyecto es:

Implementar un servidor VPN con integración de seguridad Latch, montado en una Raspberry Pi para el cifrado de información por medio de un túnel de datos para la empresa Reporne S.A.

**Actividades realizadas:**

**Fase 1. –** Se realizó una revisión de las necesidades que requería la empresa a nivel de comunicaciones donde se detectó que los usuarios que viajaban tenían que llamar para delegar sus tareas a fin de que sean cumplidas sin retrasos, así mismo que no existía un método para que puedan conectarse a la oficina en caso de temas emergentes que solo podían ser atendidos por dicho colaborador; por ello el líder de infraestructura procedió a dar la autorización formal para el desarrollo de la implementación.

**Fase 2. –** Se procedió a elaborar el capítulo 2, donde se detalló las herramientas a utilizar tanto para el hardware, como el software que brindará los mecanismos necesarios para la creación de la VPN, junto con sus métodos de seguridad, conexión y encriptación.

**Fase 3. –** Se levantó información de los colaboradores mediante una encuesta a todo el universo muestral debido a que solo existen 23 beneficiados directos en la compañía y con dichos resultados se procedió con la elaboración del capítulo 3.

**Fase 4. –** Se realiza la implementación de los servicios propuestos y las respectivas pruebas que serán adicionadas como evidencia en el presente proyecto para la revisión de los alcances propuestos.

**Objetivos específicos del proyecto:**

- Acceder a los equipos de la empresa mediante conexión remota, permitiendo trabajar desde cualquier equipo autorizado con conexión a Internet activa.

- Asegurar la comunicación entre un dispositivo externo autorizado y la red corporativa de la empresa Reporne S.A utilizando la herramienta Latch.

- Brindar la documentación necesaria para la creación de una red VPN sobre equipos Raspberry.

**Resultados propuestos:**

Al momento de implementar el servidor OpenVPN se busca crear un medio donde se pueda establecer una conexión remota que permita a los colaboradores conectarse desde los diferentes puntos del país o del exterior, donde puedan encontrarse debido a las directrices establecidas por la empresa, y que, mediante equipos autorizados, tengan acceso de

manera segura y confidencial para realizar las operaciones necesarias designadas por la compañía a fin de cumplir las métricas y objetivos de la misma.

1. **Actividades y metas:**

    - En base a la encuesta se determinó la necesidad de crear un método de acceso remoto, donde se requiere que el mismo sea seguro, rápido y confidencial, donde se salvaguarde la información sensible de la empresa y que solo sea instalado en los equipos provistos por la empresa.

    - La meta es instalar en los equipos autorizados, provistos por la empresa para los colaboradores, los certificados digitales que permitan a dichos dispositivos conversar con el servidor, establecer comunicación y ser parte de la red interna, para realizar las diferentes actividades que dependerán del área a la que pertenezca el usuario.

**¿Por qué usar OpenVPN?**

OpenVPN es un software libre que permite crear conexiones seguras a través de SSL ofreciendo una conectividad con riqueza de características a nivel empresarial, de fácil uso. Es un software multiplataforma,

pudiéndose usar en sistemas operativos Windows, Mac y Linux para dispositivos de oficina; y Android, iOS y ARM para dispositivos móviles.

Dentro de las opciones existentes de tecnologías VPN, OpenVPN es la más confiable, una de las más seguras y rápidas que existen en el mercado; su configuración e instalación no es muy compleja, se detallan dichas características en el cuadro 17.

**CUADRO 17. COMPARATIVO DE TECNOLOGIAS VPN**

| |  |  |  |
|---|---|---|---|
| **Introducción** | Un protocolo VPN muy básico, basado en PPP. La especificación PPTP en realidad no describe características de cifrado o autenticación y se basa en el protocolo PPP que se tuneliza para implementar la funcionalidad de seguridad. | Un protocolo avanzado formalmente estandarizado en IETF RFC 3193 y en la actualidad el reemplazo recomendado para PPTP en plataformas de Microsoft donde se requiere el cifrado seguro de datos. | Una solución avanzada VPN de código abierto respaldada por 'OpenVPN technologies' y que de hecho es ahora el estándar en el espacio de red de código abierto. Utiliza el protocolo de cifrado comprobado SSL/TLS. |
| **Cifrado** | La carga PPP se cifra utilizando el protocolo de cifrado punto a punto de Microsoft (MPPE). MPPE implementa el algoritmo de cifrado RSA RC4 con un máximo de 128 bits claves de sesión. | La carga útil L2TP se cifra utilizando el protocolo IPsec estandarizado. RFC 4835 especifica el algoritmo de codificación 3DES o AES para la confidencialidad. IVPN utiliza el algoritmo AES con claves de 256 bits. (AES-256 es el primer código accesible al público y cifrado abierto aprobado por la NSA para información secreta). | OpenVPN utiliza la librería OpenSSL para proporcionar cifrado. OpenSSL soporta una serie de algoritmos criptográficos diferentes como 3DES, AES, RC5, Blowfish. Al igual que con IPsec, IVPN implementa el algoritmo AES extremadamente seguro con claves de 256 bits. |

| | | | |
|---|---|---|---|
| **Debilidades en seguridad** | La implementación de Microsoft de PPTP tiene graves vulnerabilidades de seguridad. MSCHAP-v2 es vulnerable al ataque de diccionario y el algoritmo RC4 está sujeto a un ataque de bits. Microsoft recomienda encarecidamente actualizar a IPsec donde la confidencialidad es una preocupación. | IPsec no tiene vulnerabilidades principales conocidas y generalmente se considera seguro cuando se usa con un algoritmo de cifrado seguro tal como AES. Sin embargo, las presentaciones de filtraciones de la NSA indican que IKE está siendo explotado de una manera desconocida para descifrar el tráfico IPsec. También debe tenerse en cuenta que cuando IPsec está configurado para utilizar claves pre-compartidas que se hacen públicas (común con los servicios VPN públicos), es vulnerable a un ataque MITM activo. Esto no es una vulnerabilidad del protocolo IPsec sino de la forma en que se implementa. | OpenVPN no tiene mayores vulnerabilidades y se considera extremadamente seguro cuando se utiliza con un algoritmo de cifrado seguro como AES. |
| **Velocidad** | Con las claves RC4 y 128 bits, la sobrecarga de encriptación es la menos importante de los tres protocolos, lo que lo hacen PPTP el más rápido. | L2TP / IPSEC tiene una sobrecarga ligeramente superior a sus rivales debido a la doble encapsulación. Comparable a OpenVPN en la mayoría de las condiciones. | Cuando se utiliza en su modo UDP predeterminado en una red fiable, OpenVPN debe funcionar mejor que L2TP/IPsec. |
| **Puertos** | PPTP utiliza el puerto TCP 1723 y GRE (protocolo 47). PPTP puede bloquearse fácilmente restringiendo el protocolo GRE. | L2TP/IPSEC utiliza UDP 500 para el intercambio inicial de claves, protocolo 50 para los datos cifrados IPSEC (ESP), UDP 1701 para la configuración inicial L2TP y UDP 4500 para recorrido NAT. L2TP/IPsec es más fácil de bloquear que OpenVPN debido a su dependencia de protocolos fijos y puertos. | OpenVPN puede ser fácilmente configurado para ejecutarse en cualquier puerto utilizando UDP o TCP. Para evitar los cortafuegos restrictivos, OpenVPN se puede configurar para usar en el puerto 443 TCP. |

| | | | |
|---|---|---|---|
| **Instalación / Configuración** | Todas las versiones de Windows y la mayoría de los otros sistemas operativos (incluyendo móviles) tienen soporte nativo para PPTP. PPTP solo requiere un nombre de usuario, una contraseña y una dirección de servidor que lo hacen increíblemente sencillo de instalar y configurar. | Todas las versiones de Windows desde 2000 / XP y Mac OSX 10.3+ y la mayoría de los sistemas operativos móviles tienen soporte nativo para L2TP/IPsec. | OpenVPN no está incluido en ninguna versión de sistema operativo y requiere la instalación del software cliente. Los instaladores de software son muy fáciles de usar y la instalación suele tardar menos de 5 minutos. La interfaz de instalación es intuitiva. |
| **Estabilidad / Compatibilidad** | PPTP no es tan confiable, ni se recupera tan rápidamente como OpenVPN sobre conexiones de red inestables. Posee pequeños problemas de compatibilidad con el protocolo GRE y algunos enrutadores. | L2TP/IPsec es más complejo que OpenVPN y puede ser más difícil de configurar para conexiones confiables entre los dispositivos detrás de enrutadores NAT. Sin embargo, siempre y cuando tanto el servidor como el cliente soporten NAT transversal, los problemas se reducen. En la práctica, L2TP/IPsec se ha mostrado tan fiable y estable como OpenVPN para los clientes de IVPN. | Muy estable y rápido sobre redes inalámbricas, celulares y otras no confiables donde la pérdida de paquetes y la congestión es común. OpenVPN tiene un modo TCP para conexiones poco confiables, pero este modo sacrifica cierta velocidad debido a la ineficiencia al momento de encapsular TCP dentro de TCP. |
| **Plataformas** | - Windows<br>- MacOS<br>- Linux<br>- Apple iOS<br>- Android<br>- DD-WRT | - Windows<br>- MacOS<br>- Linux<br>- Apple iOS<br>- Android | - Windows<br>- MacOS<br>- Linux<br>- Apple iOS<br>- Android<br>- DD-WRT (con el firmware adecuado) |
| **Veredicto final** | Debido a las principales fallas de seguridad, no hay ninguna buena razón para elegir PPTP distinta de la compatibilidad del dispositivo. Si se tiene un dispositivo en el que no se admita L2TP/IPsec u OpenVPN, quizá puede ser una opción razonable. Si la instalación rápida y la configuración sencilla son una preocupación, entonces debe considerarse L2TP/IPsec. | L2TP/IPsec es una excelente opción, pero debido a recientes filtraciones, su seguridad puede verse comprometida. Si está utilizando un dispositivo móvil que ejecute iOS (iPhone) o Android, entonces es el más rápido de instalar y configurar, ya que es compatible de forma nativa. Sin embargo, L2TP/IPsec no debe utilizarse con claves pre-compartidas en las que la seguridad es importante. | OpenVPN es la mejor opción para todas las plataformas. Es extremadamente rápido, seguro y confiable. Además, la red IVPN Multihop sólo está disponible cuando se conecta a través de OpenVPN. El único inconveniente menor, es el requisito de instalar el software cliente, pero en la mayoría de las plataformas esto sólo toma unos minutos. |

**Elaboración:** Edwin Eduardo Sánchez Estrada
**Fuente:** https://www.ivpn.net/pptp-vs-l2tp-vs-openvpn

**¿Por qué utilizar Latch?**

Latch es un servicio que permite añadir un nivel adicional de seguridad a cuentas digitales, tales como Facebook, Twitter, Google, Dropbox, entre otros, sin embargo, no es el único del mercado, por lo cual se realizó un comparativo con otra aplicación ya existente y del gigante Google; el cliente Google Authenticator. La información se detalla en el cuadro 18.

**CUADRO 18. COMPARATIVO DE APLICATIVO TOTP**

| | Latch | |
|---|---|---|
| Alertas de acceso | Latch muestra alertas de acceso exitosos y no exitosos en cada momento que existan un evento. | Una vez que ingresa de manera correcta, Google Authenticator no genera alertas cuando existan intento fallidos posteriores. |
| Activación / Inactivación de servicios | Con Latch se puede bloquear / desbloquear un servicio solo con deslizar el dedo al abrir la aplicación, más cómodo, más rápido | Google Authenticator para bloqueo / desbloqueo, solicita código de seguridad en cada intento realizado. |
| Compatibilidad de servicios | Latch está aumentando su cartera de clientes, entre ellos Facebook, Twitter, WordPress, Dropbox, Tuenti (España), entre otros. | Google Authenticator, debido a su marca tiene a muchas empresas aliadas y su compatibilidad con ellas es mayor que la de Latch. |
| Movilidad | Latch se configura fácilmente en la mayoría de sistemas operativos. Android, iOS, Firefox OS, Windows para móviles. | Google se encuentra por defecto en Android, puesto que es dueño de dicho sistema operativo, pero no tiene compatibilidad con Firefox OS, por ejemplo. |
| Configuración / Uso | Latch es fácil de configurar y es similar en la mayoría de servicios con los que tiene convenio. En el caso de OpenVPN, se configura de manera sencilla. | Google Authenticator no maneja un estándar, es complicado y tedioso de configurar. En el caso de OpenVPN es más tediosa la configuración y se requiere solicitar varias veces código TOTP. |

| | | |
|---|---|---|
| Documentación | Latch no tiene mucha documentación, sin embargo, al ser creado por Telefónica España, tiene más contenido en español | Al igual que Latch, no existe mucha documentación, y la existente, se encuentra en su mayoría en inglés. |
| Utilidad | Latch cuenta con aplicaciones internas nativas como el TOTP (Time-based One-Time Password). En caso de registro de cuentas como Gmail, no se visualiza el usuario, dándole seguridad ante robo de credenciales. | Google Authenticator utiliza aplicaciones de terceros para ciertas funcionalidades, entre ellas TOTP. En el caso de cuentas como Gmail, aparece el nombre de usuario, haciendo la tarea de robar credenciales, más fácil. |
| Seguridad | En Latch las cuentas se generan con un Token único por dispositivo, lo que permite llevar un control de los dispositivos asociados e identificar claramente desde donde se realiza una autenticación. | Cuando se configura un código TOTP en Google Authenticator, realmente al servidor cuantos dispositivos han capturado esa semilla. Es decir, se podría tener registrada la misma cuenta en 4 dispositivos diferentes de manera insegura. |

**Elaboración:** Edwin Eduardo Sánchez Estrada
**Fuente:** Datos de la investigación

En base a los pilares de Alertar de conexión, configuración y uso, documentación existente y, sobre todo, seguridad, se procede a escoger Latch para la implementación del presente proyecto.

### ¿Cuáles son los beneficios de utilizar una VPN?

Al utilizar una red privada virtual, el colaborador que se encuentra fuera de la empresa físicamente, podrá tener acceso a las siguientes herramientas para la gestión correcta de sus funciones.

## CUADRO 19. FUNCIONALIDADES ABARCADAS POR LA VPN

| Funcionalidad | Descripción | Beneficiados |
|---|---|---|
| Acceso remoto | Permite el acceso a equipos de la empresa con la opción de escritorio remoto habilitado o mediante la aplicación VNC Viewer para brindar mayor seguridad a dichas conexiones. | Sistemas<br>Producción<br>Infraestructura |
| Acceso a aplicativos internos | Utilización de aplicaciones nativas de la empresa para generación, visualización y descarga de reportes. | Operaciones<br>Producción<br>Comercial<br>Administración<br>Financiero<br>Gerencia<br>Recursos Humanos |
| Acceso a los servicios VoIP | Utilización de la red VoIP de la empresa para uso de extensiones SIP atendiendo de manera transparente los requerimientos telefónicos. | Operaciones<br>Sistemas<br>Producción<br>Comercial<br>Administración<br>Financiero<br>OyM<br>Gerencia<br>Infraestructura<br>Recursos Humanos |
| Acceso al servidor de correo electrónico | Uso del correo electrónico empresarial para revisión, contestación y gestión de actividades y requerimientos. | Operaciones<br>Sistemas<br>Producción<br>Comercial<br>Administración<br>Financiero<br>OyM<br>Gerencia<br>Infraestructura<br>Recursos Humanos |
| Uso de internet | Utilización de internet seguro para realizar transacciones bancarias empresariales seguras, pago a proveedores y transferencias al Banco Central. | Financiero<br>Gerencia<br>Recursos Humanos |
| Acceso a servidores de test | Utilización de equipos de pre-producción para realizar pruebas de integración con nuevos clientes y/o proveedores. | Sistemas<br>Infraestructura |

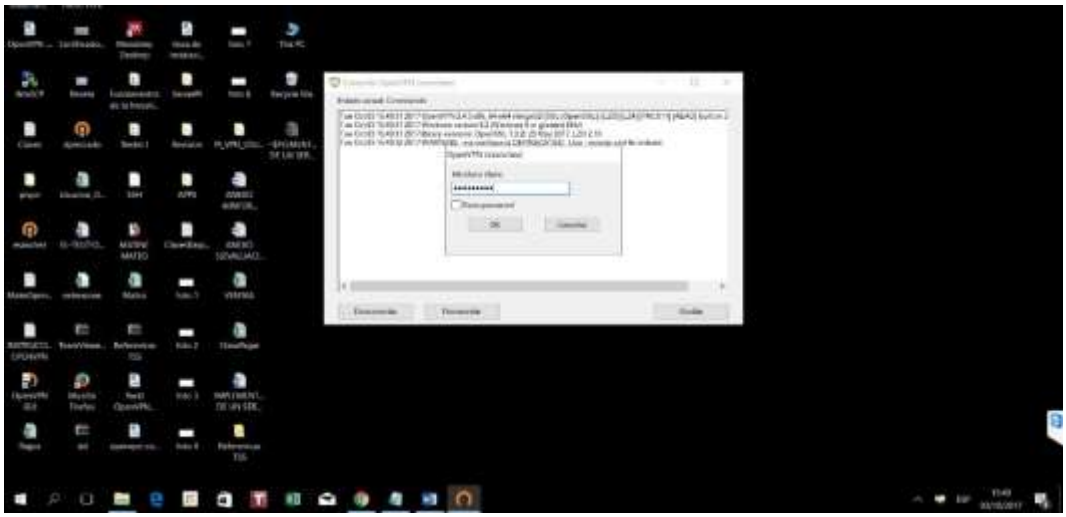
| | | |
|---|---|---|
| Acceso a cámaras IP | Revisión de videos, cámara en vivo de toda la empresa, según se requiera. | Administración<br>Gerencia<br>Recursos Humanos |
| Seguridad en el acceso | Con la aplicación Latch el administrador de Infraestructura podrá habilitar el servicio para que se utilice 24/7 (Latch inactivo) o con previa autorización (Latch activo). | Sistemas<br>Infraestructura |
| Acceso a carpetas compartidas | Revisión de información, manuales, archivos e informes almacenados en la red NAS de empresa. | Operaciones<br>Sistemas<br>Producción<br>Comercial<br>Administración<br>Financiero<br>OyM<br>Gerencia<br>Infraestructura<br>Recursos Humanos |

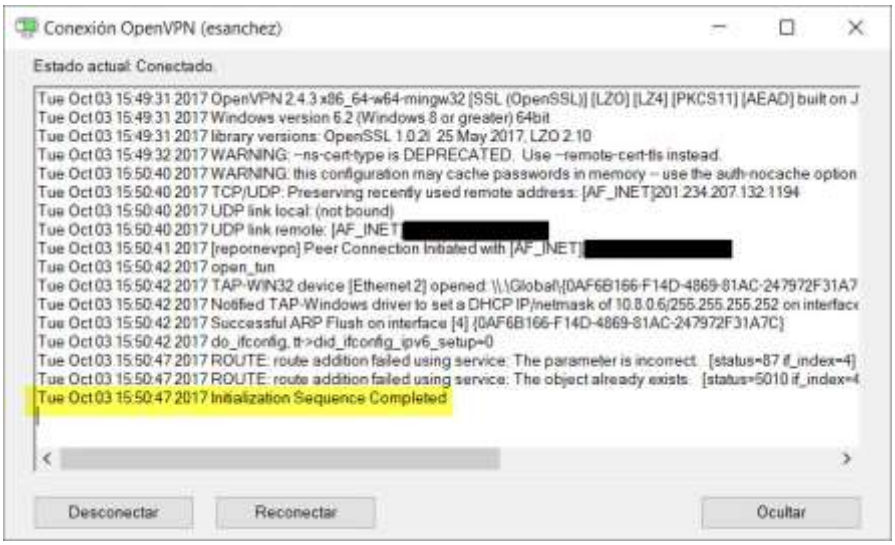
**Elaboración:** Edwin Eduardo Sánchez Estrada
**Fuente:** Datos del proyecto

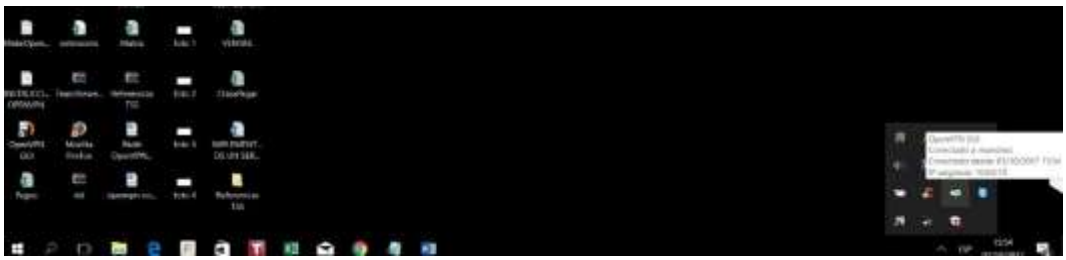
**Pruebas realizadas luego de implementación**

En base a las funcionalidades antes presentadas, se procede a realizar las respectivas pruebas donde se validarán los accesos establecidos desde una sede remota; primero se procede a establecer conexión mediante el aplicativo OpenVPN GUI:

## GRÁFICO 25. ESTABLECIMIENTO DE CONEXIÓN OPENVPN





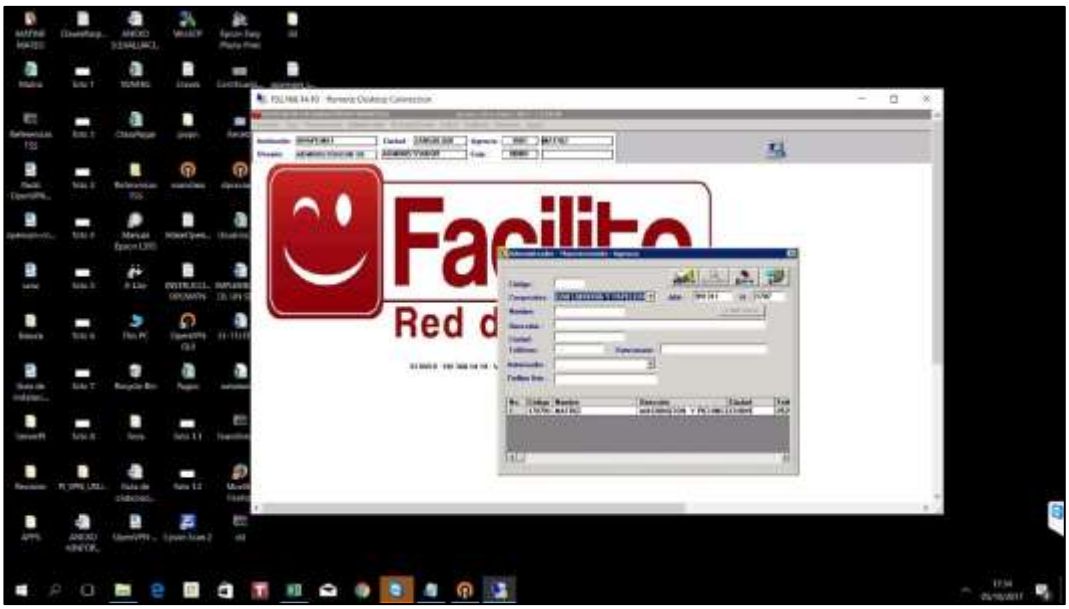
**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

**Acceso remoto**

Se realiza la prueba de acceso remoto conectándose al servidor 192.168.14.10 de la empresa:

**GRÁFICO 26. ACCESO REMOTO A SERVIDOR**



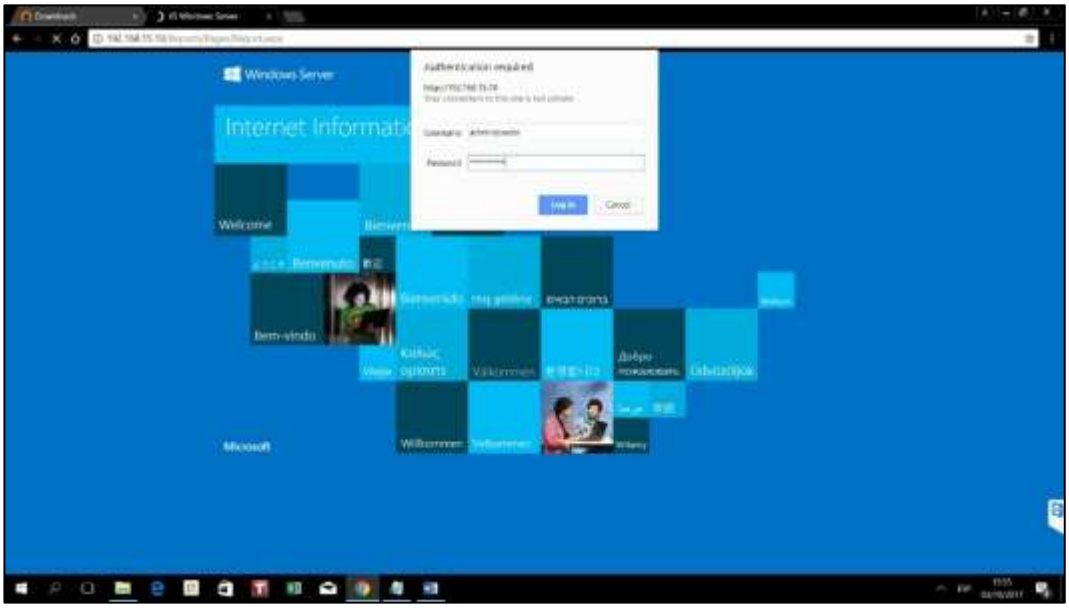
**Elaborado por:** Edwin Sánchez Estrada

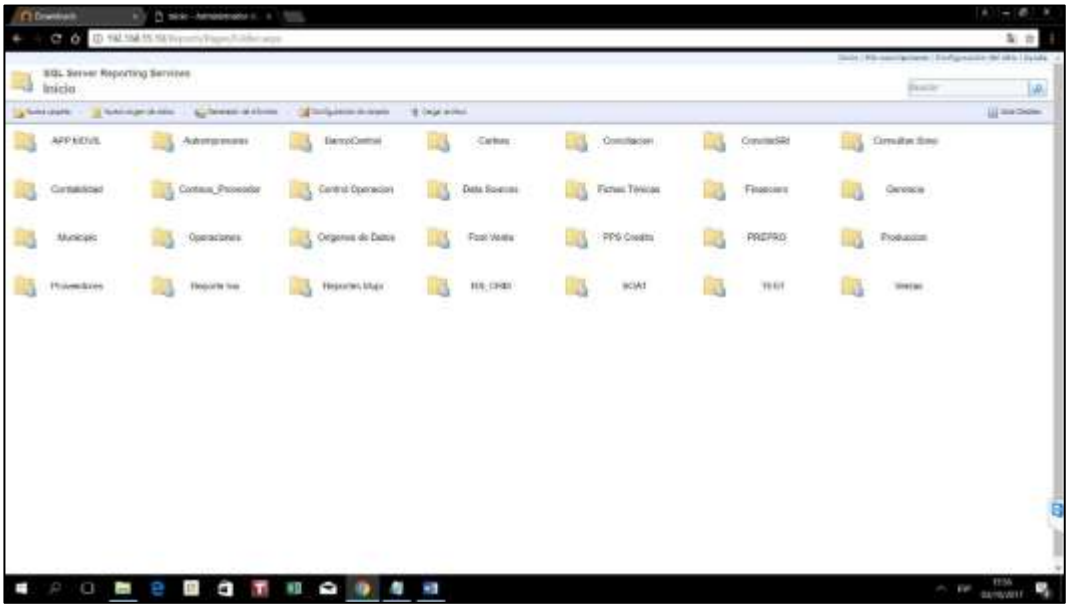
**Fuente:** Datos del proyecto

**Acceso a aplicativos internos**

La prueba de acceso a aplicaciones internas se ejecuta mediante la página http://192.168.15.10/Reports/Pages/folder.aspx, donde se pueden obtener diferentes reportes de la empresa:

**GRÁFICO 27. ACCESO A APLICATIVOS INTERNOS**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

**Acceso a los servicios VoIP**

Mediante el uso de la aplicación X-Lite, se realiza la prueba de conexión con la red VoIP de la empresa, realizando llamadas a extensiones internas:

**GRÁFICO 28. ACCESO A LA RED VOIP**

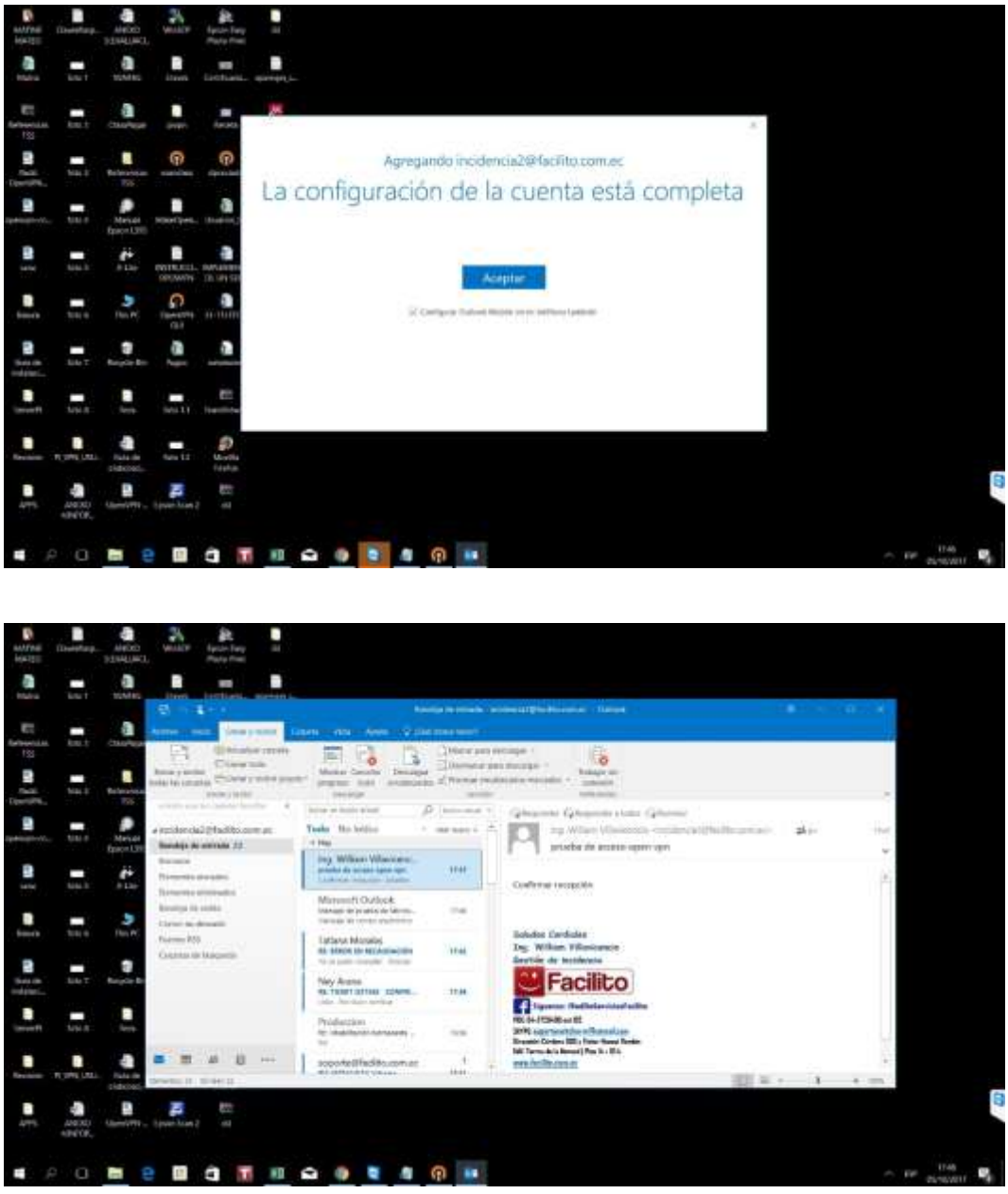
**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

**Acceso al servidor de correo electrónico**

Se realiza la prueba de conexión al servidor de correo electrónico mediante la configuración y envío/recepción de un correo electrónico:

## GRÁFICO 29. ACCESO AL SERVIDOR DE CORREOS




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

**Uso de internet**

Se procede a realizar la consulta de la página http://facilito.com.ec/facilitoweb para verificar el acceso a internet:

**GRÁFICO 30. ACCESO A INTERNET DE LA EMPRESA**

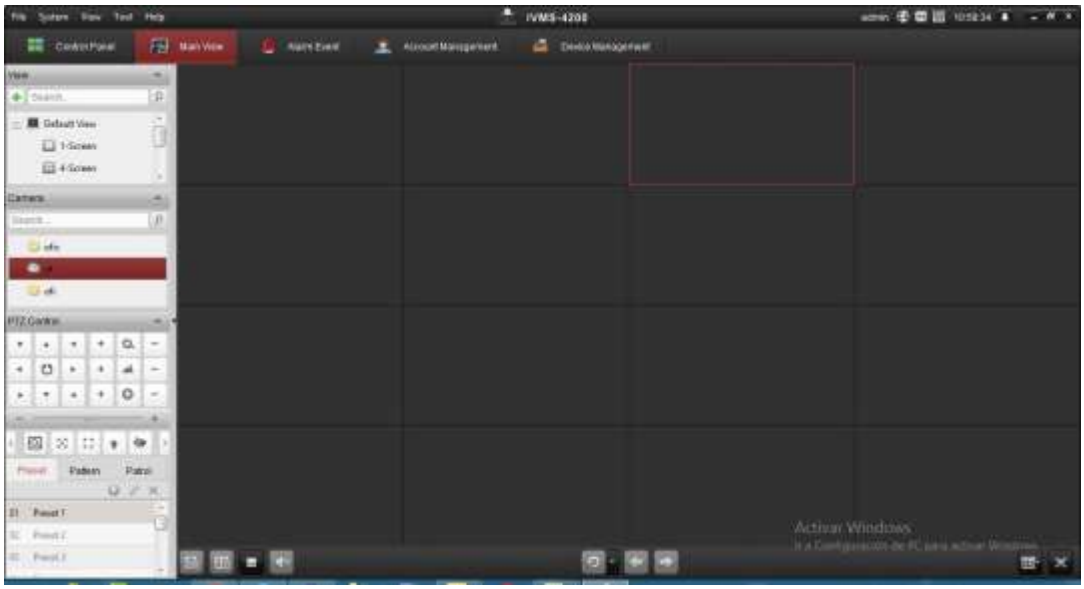

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

**Acceso a cámaras IP**

Se realiza captura de pantalla de la aplicación de cámaras IP registradas en la empresa. Por cuestiones de seguridad no se adiciona imágenes de la compañía.

**GRÁFICO 31. ACCESO A CÁMARAS IP**



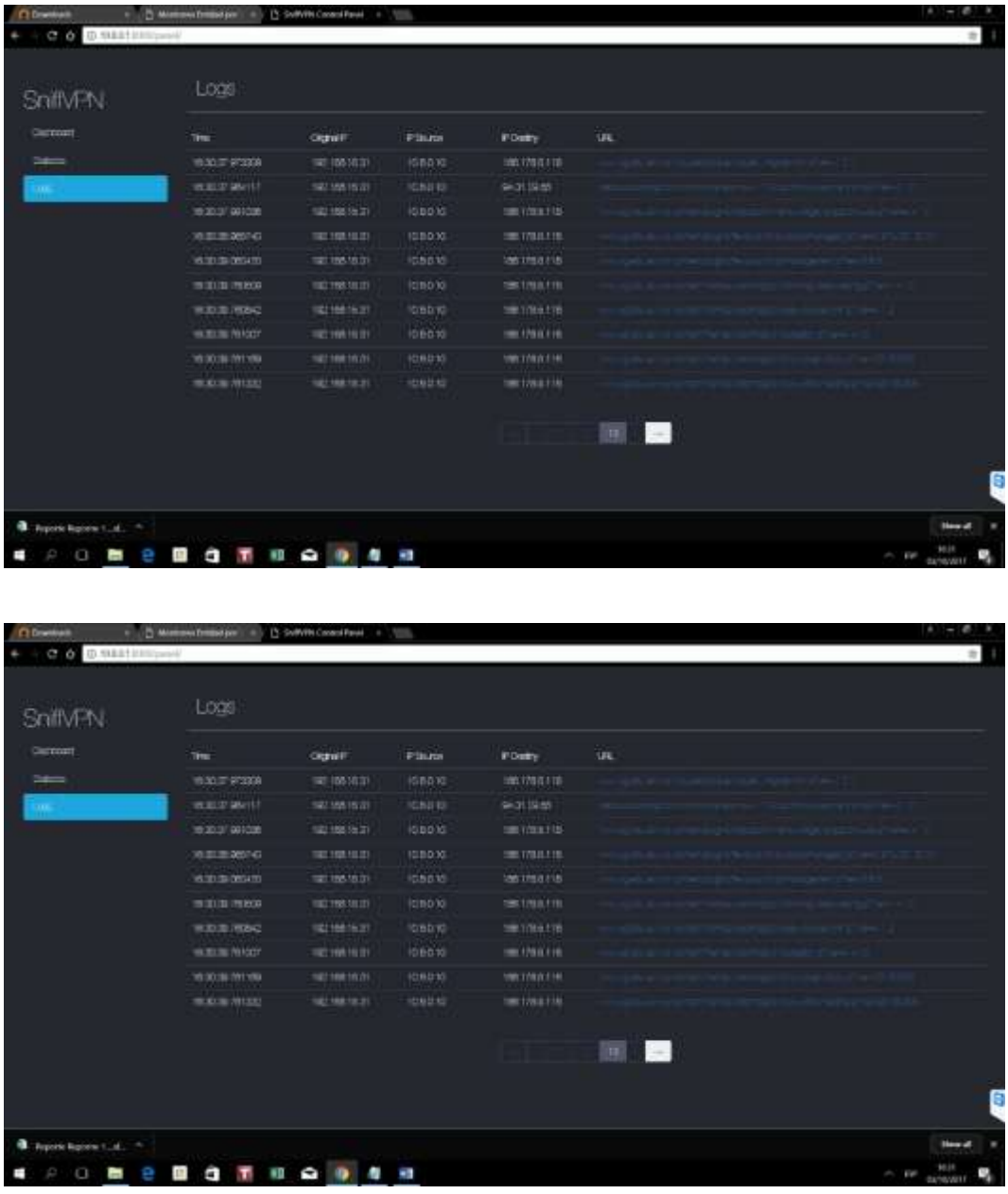
**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

**Seguridad en el acceso**

Se evidencia el escaneo de página visitadas con SniffVPN y el análisis realizado por VirusTotal donde se visualizan los registros y las url inseguras.

**GRÁFICO 32. MONITOREO DE ACCESO A PÁGINAS CON SNIFFVPN**



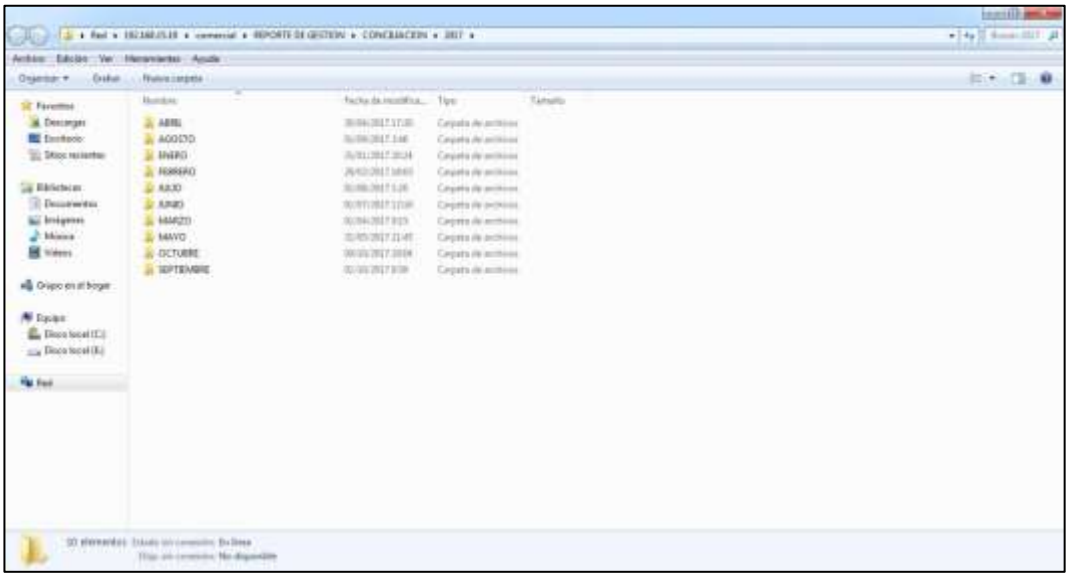

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

**Acceso a carpetas compartidas**

La red virtual permite también el acceso a recursos compartidos alojados en la red NAS:

**GRÁFICO 33. ACCESO A CARPETAS COMPARTIDAS**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** Datos del proyecto

# ANÁLISIS DE LA FACTIBILIDAD

Después de realizar la respectiva encuesta y el previo análisis de los departamentos involucrados en la empresa Reporne S.A., se determinó el presente proyecto como factible ya que se prevé mejorar la comunicación empresarial desde sitios remotos y atención de requerimientos, de manera rápida, confiable y segura; brindando a los colaboradores que posean cargos administrativos y se encuentren autorizados por el departamento de Tecnología de la Información e infraestructura, una herramienta con la capacidad de interconectarse a la red de la compañía. Su configuración es sencilla, tanto desde computadores portátiles, como dispositivos móviles, puesto que solo es necesario ingresar la contraseña, previamente establecida y el equipo se conectará en cuestión de segundos a la red empresarial.

## Factibilidad operacional

Luego de ejecutar de manera exitosa el análisis de factibilidad operacional con los departamentos de la empresa beneficiados con el proyecto, se constató la apertura y apoyo necesario para la ejecución de esta implementación que suplirá un requerimiento que en la actualidad no había sido contemplado.

Se debe tener presente que los usuarios mostraron su interés por esta herramienta que para algunos de ellos era desconocida; tenían en mente que una solución que les permita utilizar las aplicaciones de la oficina fuera de ella tenía un costo elevado para su implementación y por ello lo consideraban no viable.

La inseguridad, en la actualidad, se encuentra en todos los niveles, tanto internos como externos, y salvaguardar la información sensible, es una de las mayores premisas para la empresa y sus colaboradores; por lo cual la seguridad que se brinda con esta tecnología fue crucial para decidirse por ella; también su sencillez al momento de quererse conectar mediante las aplicaciones cliente instaladas en los diferentes dispositivos que fueron previamente autorizados.

**Factibilidad técnica**

A partir de la necesidad de los usuarios, se realizó el conversatorio con el área técnica de la empresa donde se concedió todas las facilidades para proceder con el levantamiento de información de los colaboradores, el tipo de dispositivo que utilizan, y la autorización para la instalación de los aplicativos clientes en dichos equipos.

También se dio a conocer el esquema actual de la red y el área de IT procedió a brindar una IP estática dentro de la red que tendrá acceso

limitado a las aplicaciones y equipos que el administrador del área considere necesarias.

La empresa ya cuenta con conexiones VPN que se utilizan para conexión con autorizadores, mediante protocolo L2TP/IPsec, el cual es realizado a nivel de firewall empleando un esquema punto a punto, sin embargo, para los usuarios internos no existía algún mecanismo que permita establecer comunicación bajo el modelo cliente/servidor desde equipos portátiles; por ende la propuesta de implementación parte desde cero, con la adquisición de equipos nuevos y software no instalado en la actualidad en la red empresarial.

**Factibilidad legal**

Luego del análisis realizado sobre el tema propuesto, las herramientas de hardware y el software a emplearse, se llegó a la conclusión que el presente proyecto no va en contra de ninguna norma legal vigente establecida en la constitución del Ecuador, ni de los códigos, leyes o estatus existentes en la justicia ecuatoriana; tampoco existe violación por adulteración de licencia puesto que se usa software libre para su instalación, implementación y ejecución, tanto del sistema operativo como

de las herramientas adicionales utilizadas en el proyecto, las cuales son de acceso público y gratuito dentro de la Internet.

### Factibilidad económica

Se realizó el análisis de la factibilidad económico según el costo de los equipos de hardware y software a emplearse, dando como resultado un proyecto factible y económico en comparación con un equipo de características servidor, lo cual es demostrado en el presupuesto levantado. Además, el objetivo de implementar este proyecto va en función de mantener a la empresa comunicada evitando perdidas económicas por falta de respuesta a temas surgidos con las franquiciadas de la compañía, o a su vez, perder clientes que pueden desertar debido a que sus peticiones no sean atendidas con la celeridad que corresponde.

## ETAPAS DE LA METODOLOGÍA DEL PROYECTO

### Entregables del proyecto

Los entregables del proyecto son:

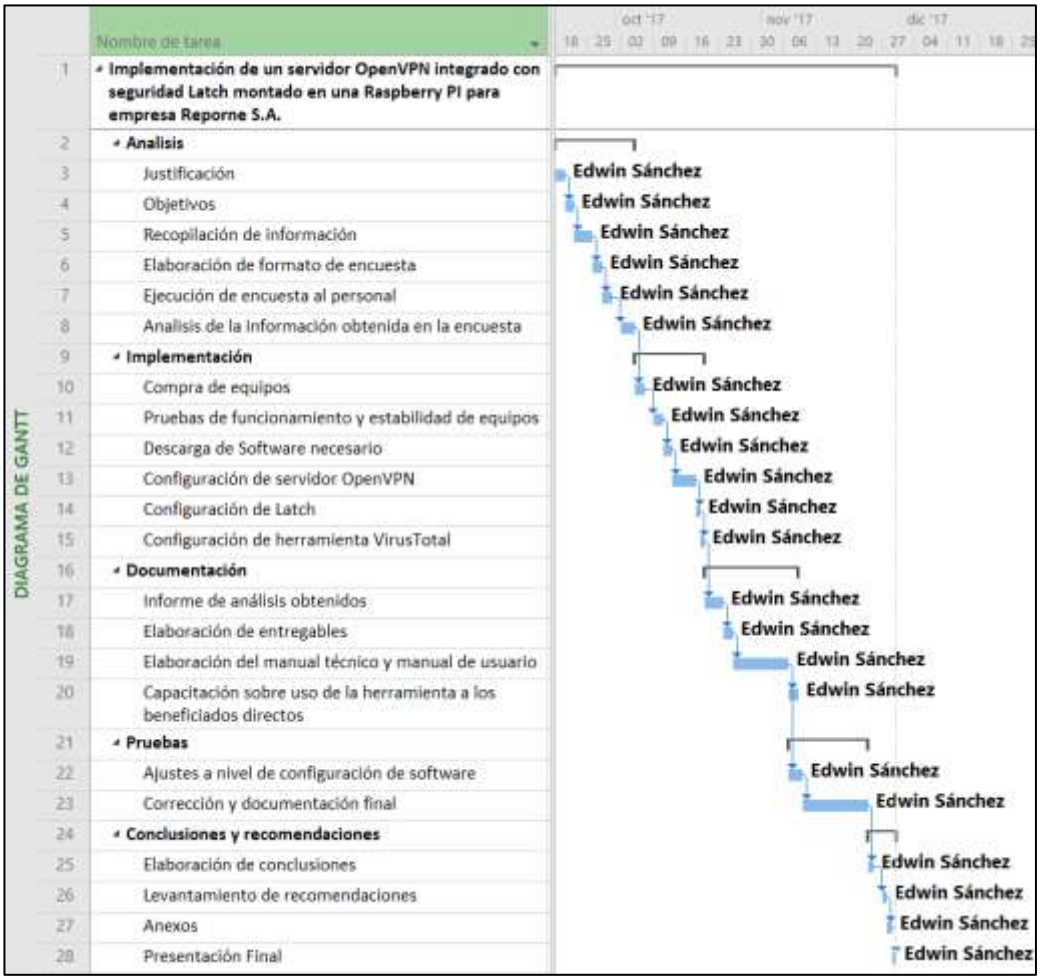
- Servidor VPN montado en Raspberry Pi, implementado.
- Manual técnico para instalación y configuración del servidor.
- Manual de usuario para clientes
- Acta de aceptación del proyecto.

## Cronograma

En el siguiente cronograma se detallan las fases que tuvo el proyecto desde el análisis de la problemática, la recopilación y análisis de la información; de esta manera se puede gestionar de manera eficiente la implementación del proyecto propuesto y abarcar los periodos de desarrollo y pruebas antes de su posterior pase a la fase de producción.

**GRÁFICO 34. CRONOGRAMA DE ACTIVIDADES**

| | Nombre de tarea | Duración | Comienzo | Fin | Predecesor | Nombres de los recursos |
|---|---|---|---|---|---|---|
| 1 | **Implementación de un servidor OpenVPN integrado con seguridad Latch montado en una Raspberry PI para empresa Reporne S.A.** | **53 días** | **lun 18/09/17** | **mié 29/11/17** | | |
| 2 | **Analisis** | **13 días** | **lun 18/09/17** | **mié 04/10/17** | | |
| 3 | Justificación | 2 días | lun 18/09/17 | mar 19/09/17 | | Edwin Sánchez |
| 4 | Objetivos | 2 días | mié 20/09/17 | jue 21/09/17 | 3 | Edwin Sánchez |
| 5 | Recopilación de información | 2 días | vie 22/09/17 | lun 25/09/17 | 4 | Edwin Sánchez |
| 6 | Elaboración de formato de encuesta | 2 días | mar 26/09/17 | mié 27/09/17 | 5 | Edwin Sánchez |
| 7 | Ejecución de encuesta al personal | 2 días | jue 28/09/17 | vie 29/09/17 | 6 | Edwin Sánchez |
| 8 | Analisis de la información obtenida en la encuesta | 3 días | lun 02/10/17 | mié 04/10/17 | 7 | Edwin Sánchez |
| 9 | **Implementación** | **11 días** | **jue 05/10/17** | **jue 19/10/17** | | |
| 10 | Compra de equipos | 2 días | jue 05/10/17 | vie 06/10/17 | 8 | Edwin Sánchez |
| 11 | Pruebas de funcionamiento y estabilidad de equipos | 2 días | lun 09/10/17 | mar 10/10/17 | 10 | Edwin Sánchez |
| 12 | Descarga de Software necesario | 2 días | mié 11/10/17 | jue 12/10/17 | 11 | Edwin Sánchez |
| 13 | Configuración de servidor OpenVPN | 3 días | vie 13/10/17 | mar 17/10/17 | 12 | Edwin Sánchez |
| 14 | Configuración de Latch | 1 día | mié 18/10/17 | mié 18/10/17 | 13 | Edwin Sánchez |
| 15 | Configuración de herramienta VirusTotal | 1 día | jue 19/10/17 | jue 19/10/17 | 14 | Edwin Sánchez |
| 16 | **Documentación** | **14 días** | **vie 20/10/17** | **mié 08/11/17** | | |
| 17 | Informe de análisis obtenidos | 2 días | vie 20/10/17 | lun 23/10/17 | 15 | Edwin Sánchez |
| 18 | Elaboración de entregables | 2 días | mar 24/10/17 | mié 25/10/17 | 17 | Edwin Sánchez |
| 19 | Elaboración del manual técnico y manual de usuario | 8 días | jue 26/10/17 | lun 06/11/17 | 18 | Edwin Sánchez |
| 20 | Capacitación sobre uso de la herramienta a los beneficiados directos | 2 días | mar 07/11/17 | mié 08/11/17 | 19 | Edwin Sánchez |
| 21 | **Pruebas** | **13 días** | **mar 07/11/17** | **jue 23/11/17** | | |
| 22 | Ajustes a nivel de configuración de software | 3 días | mar 07/11/17 | jue 09/11/17 | 19 | Edwin Sánchez |
| 23 | Corrección y documentación final | 10 días | vie 10/11/17 | jue 23/11/17 | 22 | Edwin Sánchez |
| 24 | **Conclusiones y recomendaciones** | **4 días** | **vie 24/11/17** | **mié 29/11/17** | | |
| 25 | Elaboración de conclusiones | 1 día | vie 24/11/17 | vie 24/11/17 | 23 | Edwin Sánchez |
| 26 | Levantamiento de recomendaciones | 1 día | lun 27/11/17 | lun 27/11/17 | 25 | Edwin Sánchez |
| 27 | Anexos | 1 día | mar 28/11/17 | mar 28/11/17 | 26 | Edwin Sánchez |
| 28 | Presentación Final | 1 día | mié 29/11/17 | mié 29/11/17 | 27 | Edwin Sánchez |




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** El autor

**Presupuesto General de Implementación de un servidor OpenVPN integrado con seguridad Latch montado en una Raspberry Pi para la empresa Reporne S.A.**

Se adjuntan los costos a invertir dentro de la implementación del servidor OpenVPN con seguridad Latch:

## GRÁFICO 35. PRESUPUESTO DE IMPLEMENTACIÓN

| PRESUPUESTO GENERAL DE IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A. | | | | | |
|---|---|---|---|---|---|
| **DESCRIPCION DE LOS ITEMS** | **CANTIDADES** | **COSTOS UNITARIOS** | **SUBCOSTOS** | **IVA 12%** | **COSTOS UNITARIOS** |
| **1. RECURSO HUMANO** | | | | | |
| 1.1 Ingenieros en Networking y Telecomunicaciones | 1 | $ - | $ - | $ - | $ - |
| 1.2 Personal Técnico (asignado por la empresa) | 1 | $ - | $ - | $ - | $ - |
| **SUBTOTAL DE RECURSOS HUMANOS** | | | | | $ - |
| **2. RECURSO HARDWARE** | | | | | |
| 2.1 Tarjeta Raspberry PI 3 Model B | 1 | $ 60,00 | $ 60,00 | $ 7,20 | $ 67,20 |
| 2.2 Cargador 5V - 2.4A | 1 | $ 10,50 | $ 10,50 | $ 1,26 | $ 11,76 |
| 2.3 Tarjeta Memoria SanDisk Ultra microSDHC UHS-I Clase10 | 1 | $ 8,00 | $ 8,00 | $ 0,96 | $ 8,96 |
| 2.4 Carcasa para Raspberry Pi 3 | 1 | $ 10,00 | $ 10,00 | $ 1,20 | $ 11,20 |
| **SUBTOTAL DE RECURSOS HARDWARE** | | | | | $ 99,12 |
| **3. RECURSO MATERIALES** | | | | | |
| 3.1 Cable Patch cord CAT 6 | 1 | $ 2,00 | $ 2,00 | $ 0,24 | $ 2,24 |
| **SUBTOTAL DE RECURSOS MATERIALES** | | | | | $ 2,24 |
| **4. RECURSO SOFTWARE** | | | | | |
| 4.1 Sistema Operativo Raspbian Stretch Lite | 1 | $ - | $ - | $ - | $ - |
| 4.2 OpenVPN Server | 1 | $ - | $ - | $ - | $ - |
| 4.3 OpenVPN Connect - Cliente | 1 | $ - | $ - | $ - | $ - |
| 4.4 Software de seguridad adicional Latch | 1 | $ - | $ - | $ - | $ - |
| 4.5 Software de monitoreo SniffVPN + VirusTotal | 1 | $ - | $ - | $ - | $ - |
| **SUBTOTAL DE RECURSOS SOFTWARE** | | | | | $ - |
| **5. GASTOS VARIOS** | | | | | |
| 5.1 Alimentación (mensual) | 30 | $ 2,50 | $ 75,00 | $ 9,00 | $ 84,00 |
| 5.2 Útiles de Oficina | 1 | $ 25,00 | $ 25,00 | $ 3,00 | $ 28,00 |
| **SUBTOTAL DE GASTOS VARIOS** | | | | | $ 112,00 |
| **TOTAL** | | | | | $ 213,36 |

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** El autor

### Requerimientos de Hardware para la implementación del servidor

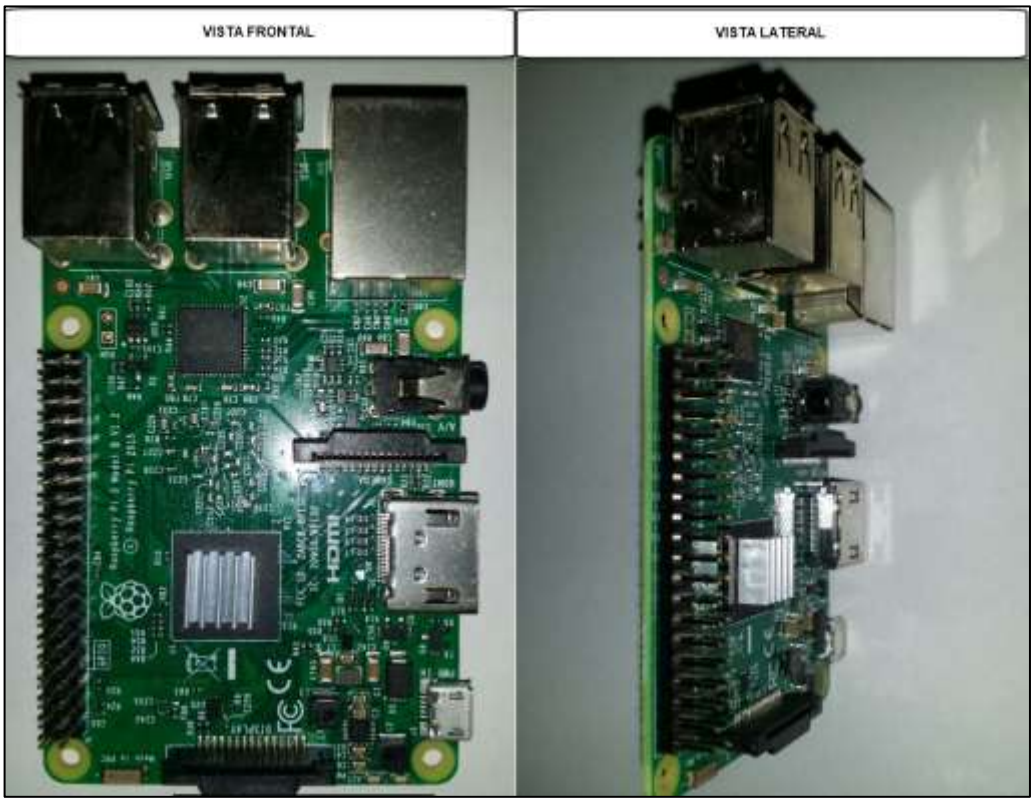
Se procede a detallar las características de hardware necesarias para la implementación del servidor VPN para conocer claramente cuáles son los recursos con los cuales se cuenta. De esta manera se podrá tener idea de la factibilidad del proyecto, además de dar una guía en caso de futuras instalaciones en un sitio distinto al descrito en este presente proyecto.

Los siguientes equipos son los necesarios para la instalación, desarrollo y ejecución del proyecto.

**Tarjeta Raspberry Pi 3 Model B**

Esta tarjeta nos sirve como equipo servidor donde se instalará posteriormente el sistema operativo y el software necesario para la gestión de la VPN.

**GRÁFICO 36. TARJETA RASPBERRY PI 3**




**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** El autor

La tarjeta basada en la tecnología ARM es una poderosa herramienta utilizada en el campo universitario y científico para creación de proyectos de diferentes ámbitos, tecnológico, científico, ambiental, entre otros.

**Tarjeta de Memoria microSD**

Se adquirió una Tarjeta Memoria SanDisk Ultra microSDHC UHS-I Clase10, puesto que con ella el desempeño de la tarjeta Raspberry es mejor, según las especificaciones del fabricante.

**GRÁFICO 37. TARJETA DE MEMORIA SANDISK**


**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** El autor

La tarjeta incluye un adaptador el cual permitirá su utilización en la laptop en la ranura SD para la carga inicial del sistema operativo.

**Case Raspberry Pi 3**

Brinda protección a la tarjeta contra posibles golpes o descargas de energía de otros equipos, no viene incluida, por lo que se tuvo que adquirir de manera adicional

**GRÁFICO 38. CASE RASPBERRY PI 3**

**Elaborado por:** Edwin Sánchez Estrada

**Fuente:** El autor

## Requerimientos de Software para la implementación del servidor

### CUADRO 20. REQUERIMIENTOS DE SOFTWARE

| Producto Software | Descripción | Propósito de Uso | Versión | Fuente |
|---|---|---|---|---|
| **Raspbian Stretch Lite** | Software Linux necesario para arrancar el equipo y los programas | Sistema Operativo donde se instalarán los diferentes aplicativos | 4.9 | https://www.raspberrypi.org/downloads/raspbian/ |
| **OpenVPN Server** | Aplicación para instalar el servidor VPN dentro del sistema operativo | Utilizada para montar el servidor y generar conexiones VPN seguros mediante el modelo cliente/servidor | 2.4.0 | https://openvpn.net/index.php/open-source/downloads.html |
| **OpenVPN Connect** | Aplicativo cliente que se instala en la maquina host para conversación con el servidor OpenVPN | Aplicación para iniciar la conexión VPN desde el Host | 11.8.0.0 | https://openvpn.net/index.php/open-source/downloads.html |
| **Latch** | Aplicativo que se instala en un móvil para el bloqueo/desbloqueo de servicios | Se aplica para brindar una capa adicional de seguridad al servicio VPN | 1.8 | https://latch.elevenpaths.com/ |
| **VirusTotal** | Software que censa la visita a sitios y detecta url con contenido maliciosos | Se aplica en la VPN para alertar sobre la visita a un sitio malicioso al administrador TI | 1.3 | https://github.com/VirusTotal/qt-virustotal-uploader |
| **Python** | Lenguaje de programación interpretado, que soporta orientación a objetos e imperativa | Base para la utilización del programa SnifferVPN que viene el software VirusTotal | 2.7.13 | https://www.python.org/downloads/release/python-2713/ |

| | | | | |
|---|---|---|---|---|
| **Apache** | Software que procesa conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas. | Utilizado para levantar la interfaz web del sitio SniffVPN de VirusTotal | 2.4.25 | https://httpd.apache.org/download.cgi |
| **Win32 Disk Imager** | Software que permite la lectura y escritura de imágenes ISO en tarjetas de memoria | Necesario para instalar la imagen del OS Raspbian Stretch Lite dentro de la Raspberry Pi | 0.9.5 | https://sourceforge.net/projects/win32diskimager/ |
| **Putty** | Software que se instala en un host y permite la conexión al servidor vía SSH | Se utiliza para realizar las configuraciones dentro del servidor mediante el protocolo SSH. | 0.69 | http://www.putty.org/ |
| **WinSCP** | Software que gestiona la transferencia de archivos desde el servidor. | Utilizado para obtener los certificados digitales y archivos para configurar el cliente. | 5.9.5 | https://winscp.net/eng/download.php |
| **Active@ KillDisk Freeware Suite** | Software que permite el formateo de tarjetas de memoria de manera sencilla. | Utilizado por dar formato a la tarjeta de memoria de manera inicial. | 10.1.1 | http://www.killdisk.com/killdisk-freeware.htm |

**Elaboración:** Edwin Eduardo Sánchez Estrada

**Fuente:** Datos de la investigación

**Criterios de validación de la propuesta**

Como criterio de validación de la propuesta, se procede a generar un informe de pruebas dentro del cual se detalla el funcionamiento adecuado del servicio dentro de los parámetros establecidos en este presente proyecto, así mismo el detalle de creación de usuarios.

**Criterios de aceptación del producto**

**CUADRO 21. CRITERIOS DE ACEPTACIÓN DEL PRODUCTO**

| **Característica/Funcionalidad** | | |
|---|---|---|
| Implementar servidor OpenVPN que permita el acceso remoto de diferentes equipos configurados pertenecientes a la empresa Reporne S.A. | | |
| **Razón/Resultado** | | |
| Interconexión de usuarios que se encuentren fuera de la oficina por temas laborales para evitar delegar el trabajo o dilatar tiempos de respuesta. | | |
| **Escenario 1** | **Criterio de aceptación (Título)** | |
| | Petición de conexión con certificado y contraseña válida | |
| | **Contexto** | Cada colaborador debe tener un usuario y contraseña personalizados creados para el acceso, se acepta la petición |
| | **Evento** | Ejecución del intento de conexión |
| | **Resultado** | Aceptación |
| **Escenario 2** | **Criterio de aceptación (Título)** | |
| | Petición de conexión con certificado válido y contraseña incorrecta | |
| | **Contexto** | En caso de que el certificado sea el correcto, pero la contraseña inválida, se rechaza la conexión. |
| | **Evento** | Ejecución del intento de conexión |
| | **Resultado** | Rechazo |
| **Escenario 3** | **Criterio de aceptación (Título)** | |
| | Petición de conexión con certificado inválido/caducado. | |
| | **Contexto** | En caso de que el certificado sea inválido o caducado, se rechaza la conexión |
| | **Evento** | Ejecución del intento de conexión |
| | **Resultado** | Rechazo |
| **Escenario 4** | **Criterio de aceptación (Título)** | |
| | Petición de conexión con problemas de comunicación | |
| | **Contexto** | En caso de que existan problemas de comunicación, la conexión se rechazará |
| | **Evento** | Ejecución del intento de conexión |

| | | |
|---|---|---|
| | **Resultado** | Rechazo |
| **Característica/Funcionalidad** | | |
| Configurar capa de seguridad adicional Latch para tener control del acceso al servicio OpenVPN en general | | |
| **Razón/Resultado** | | |
| Integrar la capa Latch que permitirá ver los intentos de conexión fallidos, bloquear o permitir el acceso al servicio en general. | | |
| **Escenario 1** | **Criterio de aceptación (Título)** | |
| | Intento de autenticación con acceso total habilitado en la aplicación. | |
| | **Contexto** | El usuario puede autenticarse sin problemas al servidor OpenVPN. |
| | **Evento** | Autenticación con el servidor VPN |
| | **Resultado** | Aceptación |
| **Escenario 2** | **Criterio de aceptación (Título)** | |
| | Intento de autenticación con bloqueo total habilitado en la aplicación. | |
| | **Contexto** | El usuario no puede autenticarse en el servidor OpenVPN, registro de alerta de intento fallido en la aplicación. |
| | **Evento** | Autenticación con el servidor VPN |
| | **Resultado** | Rechazo |
| **Característica/Funcionalidad** | | |
| Visualizar el tráfico de los clientes conectados e identificar las páginas maliciosas a las que se pueda intentar acceder. | | |
| **Razón/Resultado** | | |
| Poder conocer los usuarios que intentan acceder a una página maliciosas para su respectiva retroalimentación. | | |
| **Escenario 1** | **Criterio de aceptación (Título)** | |
| | Navegación en sitios seguros, evitando acceder a sitios maliciosos que puedan infectar la red corporativa. | |
| | **Contexto** | En caso de intentar acceder a un sitio malicioso por parte de un usuario conectado mediante la VPN. |
| | **Evento** | Administración de sitios visitados por parte de los clientes. |
| | **Resultado** | Aceptación o denegación de los servicios de red. |
| **Característica/Funcionalidad** | | |
| Administrador el servidor de forma remota por parte del administrador IT o de Infraestructura | | |
| **Razón/Resultado** | | |
| Poder revisar el estado del servidor, creación de usuarios o revocación de permisos permanentes. | | |
| **Escenario 1** | **Criterio de aceptación (Título)** | |
| | Ingreso a administración del servidor VPN, mediante protocolo SSH. | |

| | | |
|---|---|---|
| | **Contexto** | Ingreso con usuario válido y contraseña valida, y habilitación de Latch habilitada para SSH. |
| | **Evento** | Intento de conexión a la administración del servidor. |
| | **Resultado** | Aceptación |
| **Escenario 2** | **Criterio de aceptación (Título)** | |
| | Ingreso a administración del servidor VPN, mediante protocolo SSH. | |
| | **Contexto** | Ingreso con usuario válido e inválida, y habilitación de Latch habilitada para SSH. |
| | **Evento** | Intento de conexión a la administración del servidor. |
| | **Resultado** | Rechazo |
| **Escenario 3** | **Criterio de aceptación (Título)** | |
| | Ingreso a administración del servidor VPN, mediante protocolo SSH. | |
| | **Contexto** | Ingreso con usuario invalido, y habilitación de Latch habilitada para SSH. |
| | **Evento** | Intento de conexión a la administración del servidor. |
| | **Resultado** | Rechazo |
| **Escenario 4** | **Criterio de aceptación (Título)** | |
| | Ingreso a administración del servidor VPN, mediante protocolo SSH. | |
| | **Contexto** | Ingreso con credenciales válidas o inválidas, e inhabilitación de Latch habilitada para SSH. |
| | **Evento** | Intento de conexión a la administración del servidor. |
| | **Resultado** | Rechazo |

**Elaboración:** Edwin Eduardo Sánchez Estrada

**Fuente:** El Autor

# CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

En base al análisis y estudio realizado al protocolo OpenVPN y a la implementación del servidor VPN con seguridad Latch, bajo los objetivos establecidos en el proceso de levantamiento de información, desarrollo, ejecución y culminación del proyecto de titulación, se concluye lo siguiente:

- La ejecución del presente proyecto buscó crear un canal de comunicación privado donde la información de la empresa viaje por el internet de manera segura para aquellos colaboradores que por razones varias debían ausentarse de la compañía para gestionar tareas relacionadas a su área o departamento.

- Se logró acceder a los equipos de manera remota, creando también un canal de consulta de las aplicaciones propias de la empresa, donde se permite generar reportes en tiempo real para su visualización y descarga y se adicionó una capa adicional de seguridad utilizando la aplicación Latch previamente configurada y pareada en el servidor VPN.

- Se generó la documentación paso a paso para la configuración del servidor, junto con el pareo de Latch y también sobre el uso de clientes en las plataformas Windows y Android.

**Recomendaciones**

Se recomienda la consideración de los siguientes puntos:

- En la actualidad no existe ningún sistema que sea 100% infalible, puesto que siempre existirán métodos de explotación que podrán vulnerar hasta el sistema más robusto, por ello se recomienda crear conciencia a los usuarios del sistema para evitar acceder a links o llenar formularios ajenos a la empresa mientras estén conectados a la VPN, ya que pueden resultar en ataques informáticos que pueden comprometer la seguridad de la información de la misma.

- La herramienta Latch brinda seguridad de acceso adicional de diferentes servicios, como Facebook, Twitter, OpenVPN, inclusive para Windows; para este último se recomienda la exploración para su incorporación al Directorio Activo a fin de permitir la administración remota de usuarios del directorio en la red corporativa.

- La documentación presentada en este proyecto de titulación es acerca de la configuración del servidor VPN basado en una encriptación AES-256 de 2048 bits mediante llaves OpenSSL, sin embargo, no es el único método de encriptación existente, se recomienda la revisión de estos protocolos de cifrado para que se adapte a las necesidades del lugar donde se lo necesite implementar.

## BIBLIOGRAFÍA


Alvarez, D., Jorquera, C., Sepúlveda, G., & Zamora, C. (2014). Redes Privadas Virtuales (VPN), 1-15. Recuperado a partir de http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes Privadas Virtuales %28VPN%29.pdf

Crist, E. F., & Keijser, J. J. (2015). *Mastering OpenVPN*. Recuperado a partir de https://github.com/tuantm8/eBook-1/raw/master/Mastering OpenVPN (2015) (Pdf%2C Epub %26 Mobi) Gooner/Mastering OpenVPN (2015).pdf

Dubs de Moya, R. (2002). El Proyecto Factible: una módalidad de investigación. *Sapiens. Revista Universitaria de Investigación*, *3*. Recuperado a partir de http://www.redalyc.org/pdf/410/41030203.pdf

Escobar, M. (2015). *Criptografía en clave pública y privada. RSA.* Universitat Jaume. Recuperado a partir de http://repositori.uji.es/xmlui/bitstream/handle/10234/139037/TFG_2015_EcobarBenetM.pdf?sequence=1

Gonzalez, H., & Gainza, D. (2016). USING OF OPERATORS BITWISE IN WEB APPLICATIONS OF HOME AUTOMATION WITH, (March). Recuperado a partir de https://www.researchgate.net/profile/Henry_Gonzalez_Brito/publication/301359298_USING_OF_OPERATORS_BITWISE_IN_WEB_APPLICATIONS_OF_HOME_AUTOMATION_WITH_RASPBERRY_PI/links/571598ad08ae8ab56695b1eb/USING-OF-OPERATORS-BITWISE-

IN-WEB-APPLICATIONS-OF-HOME-AUTOMATION-WITH-RASPBERRY-PI.pdf

Hertzog, R., & Mas, R. (2015). *The Debian administrator's handbook*. Recuperado a partir de https://debian-handbook.info/download/es-ES/stable/debian-handbook.pdf

Ivković, J., & Radulović, B. (2016). The Advantages of Using Raspberry Pi 3 Compared to Raspberry Pi 2 SoC Computers for Sensor System Support. *Proccedings of the ICAIIT2016*, (June), 88-94. https://doi.org/10.20544/AIIT2016.12

Kula, P. J. (2014). *Raspberry Pi Server Essentials*. Recuperado a partir de http://freepdf-books.com/download/2016/03/090316/Raspberry Pi Server Essentials Book.pdf

Mansilla, C. M. (2014). Redes de computadoras. Recuperado a partir de http://www.fca.unl.edu.ar/informaticabasica/Redes.pdf

Pazmiño, V. (2013). Análisis e implementación de la mejor alternativa para una VPN de la empresa Optimsoft para interconectarla base de datos de importaciones entre Quito y Guayaquil., 1-7.

Perez, J. (2015). Control domótico con dispositivos móviles, (July). https://doi.org/10.13140/RG.2.1.5105.3922

Telefónica Digital Identity. (2015a). Manual de uso de la app Latch. Utilización con Nevele Bank., 1-44. Recuperado a partir de https://latch.elevenpaths.com/www/public/documents/howToUseLatchNevele_ES.pdf

Telefónica Digital Identity. (2015b). Manual de uso paso a paso de la app Latch con Tuenti, 1-19. Recuperado a partir de https://latch.elevenpaths.com/www/public/documents/tutorials/Guia_integracion_Latch_Tuenti_es.pdf

Upton, E., & Halfacree, G. (2016). *Raspberry Pi User Guide*. Recuperado a partir de http://ebook-dl.com/book/3714

## ANEXOS

## ANEXO N ° 1

**Formato de encuesta realizada a colaboradores de la empresa Reporne S.A.**

**UNIVERSIDAD DE GUAYAQUIL**

**FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS**

**CARRERA DE NETWORKING Y TELECOMUNICACIONES**

1. **¿Qué tan frecuentemente usted se ausenta de la empresa por motivos laborales?**

| | |
|---|---|
| Frecuentemente | |
| Ocasionalmente | |
| Nunca | |

2. **En caso de estar ausente y requerir atender o gestionar un tema urgente de la empresa, ¿Cómo procede?**

| | |
|---|---|
| Abandona la actividad que esté realizando, y acude inmediatamente a la empresa. | |
| Delega el tema a otro colaborador. | |
| El tema debe esperar hasta que usted se encuentre en la empresa. | |

3. **¿Conoce usted cómo funcionan las redes privadas virtuales o VPN?**

| | |
|---|---|
| Sí | |
| No | |

4. **¿Considera usted qué es seguro conectarse desde una red abierta o desconocida, hacia el Internet?**

| | |
|---|---|
| Sí | |
| No | |

5. **¿Cree usted qué es necesario tener un medio de conexión seguro a la empresa, para atención de temas emergentes?**

| | |
|---|---|
| Sí | |
| No | |

6. **¿En qué departamento de la empresa usted desempeña sus funciones?**

| | |
|---|---|
| Operaciones | |
| Sistemas | |

| | |
|---|---|
| Administración | |
| Financiero | |
| Comercial | |
| Recursos Humanos | |
| Otro | |

7. **¿Cuándo se encuentra fuera de la oficina, qué tan complicado es encontrar un punto de acceso a Internet?**

| | |
|---|---|
| Muy probable | |
| Poco probable | |
| Improbable | |

8. **¿Considera usted que es importante implementar métodos para evitar el robo de información cuándo existan conexiones remotas a la empresa?**

| | |
|---|---|
| Sí | |
| No | |

9. **¿Cómo evalúa usted la posibilidad de que se pueda establecer una conexión remota a la red de la empresa, para revisión de temas laborales emergentes?**

| | |
|---|---|
| Excelente | |
| Buena | |
| Mala | |
| Pésima | |

10. **¿Dispone usted de un dispositivo portátil, cómo laptop o Tablet, provisto por la empresa para uso laboral?**

| | |
|---|---|
| Sí | |
| No | |

11. **¿Qué aspectos usted prefiere de una conexión remota por VPN?**

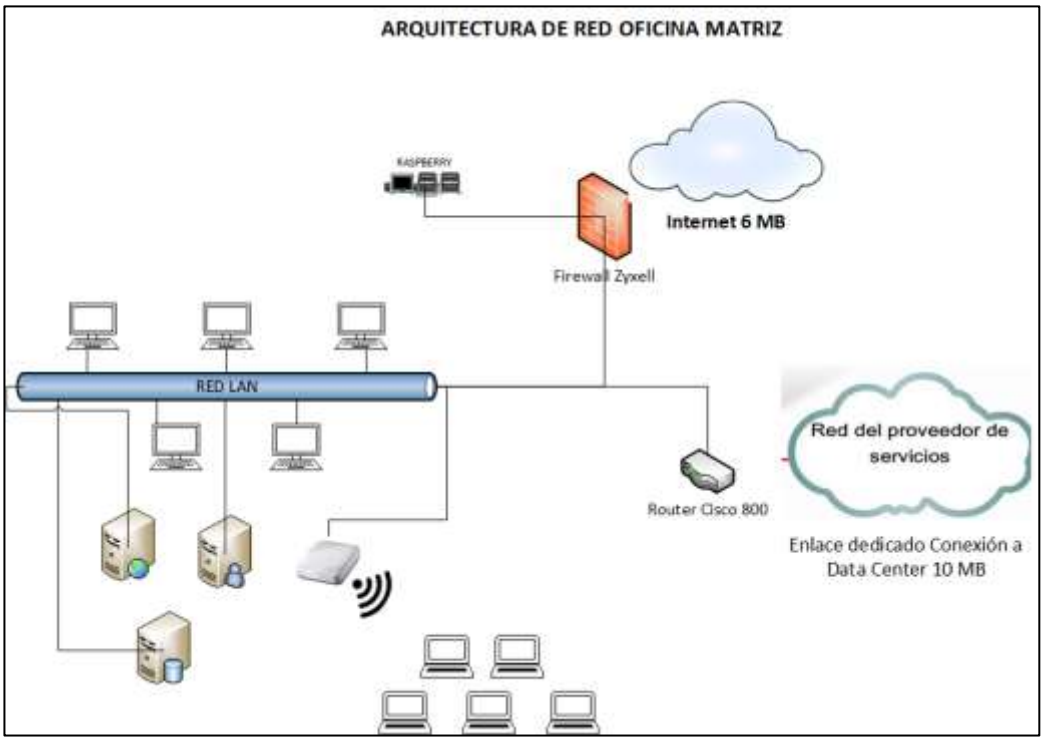
| | |
|---|---|
| Seguridad | |
| Rapidez | |
| Todas las anteriores | |

12. **Considera usted que la implementación de una conexión VPN que le permita conectarse remotamente, ayudará a mejorar la productividad de la empresa?**

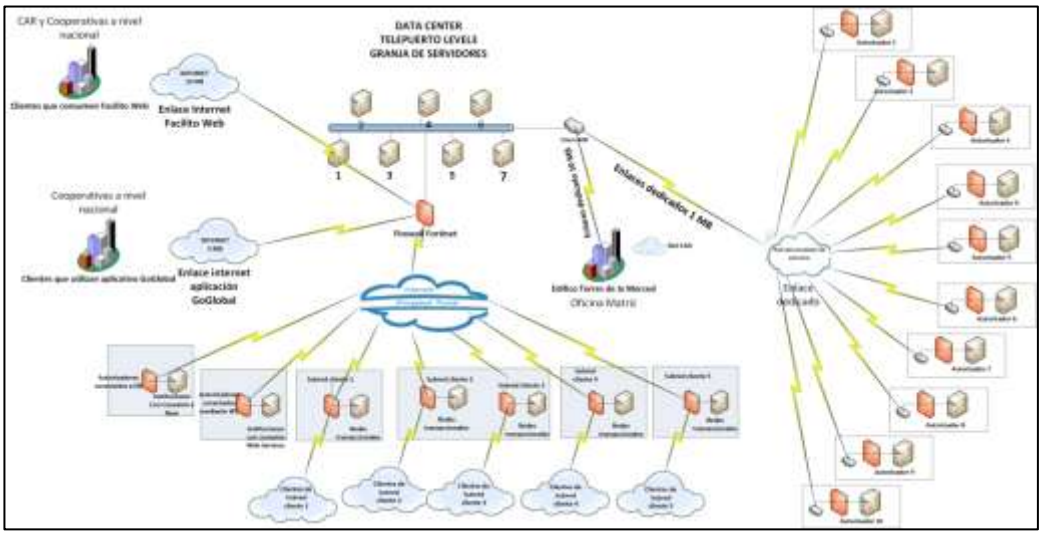
| | |
|---|---|
| Sí | |
| No | |

## ANEXO N ° 2

## Diseño de la Red Corporativa




**RED ENLACE CON DATACENTER**



## ANEXO N ° 3

## Carta de autorización para la implementación del proyecto

REPORNE S.A.

Facilito
Red de servicios

Guayaquil, 19 de junio del 2017

**Sres.**
**Universidad de Guayaquil**
**Ciudad.**

Por medio de la presente autorizo al Sr. EDWIN EDUARDO SÁNCHEZ ESTRADA, con C.I. 092315959-4, estudiante de la Carrera de Ingeniería en Networking y Telecomunicaciones, de la Facultad de Ciencias Matemáticas y Física a que proceda a desarrollar su proyecto con título:

**"IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A"**

Para lo cual se le procederá a brindar las facilidades necesarias para que ejecute dicha implementación dentro del marco legal existente en el reglamento interno correspondiente.

Atentamente

**Víctor Guerrero Zambrano**
**Líder de Infraestructura**
**Reporne S.A.**

General Córdova 808 y Víctor Manuel Rendon Edif. Torres de la Merced, Piso 14 Of 4 - Telef.: 04-372#400

## ANEXO N ° 4

## Manual técnico de configuración

**Requisitos previos para la implementación:**

Se deben tener presentes algunos requisitos antes de realizar la implementación, para que no existan inconvenientes al momento del desarrollo; las herramientas que se utilizaron se detallan a continuación:

- Laptop Toshiba Satellite con lector de Memory Card SD.
- Sistema Operativo Windows 10
- Tarjeta de memoria MicroSD SDHC 16 GB Clase 10 + adaptador SD.
- Instalar el programa Win32 Disk Imager
- Instalar el cliente Putty
- Instalar el software WinSCP
- Instalar Active@ KillDisk Freeware Suite
- Sistema operativo Raspbian Stretch Lite

### Instalación del sistema operativo

### Formateo Inicial de tarjeta de memoria

Procedemos a realizar el formateo de la tarjeta de memoria con el software **Active@ KillDisk Freeware Suite**. Para ello, procedemos a introducir la tarjeta de Memoria MicroSD, dentro del adaptador SD:

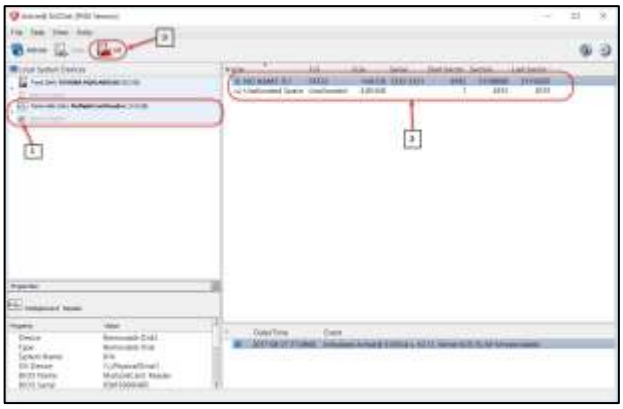
**Adaptador SD y Tarjeta MicroSD**


**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

Se presiona el botón **Refresh** para que aparezca la tarjeta que se introdujo, luego se da clic en la casilla que corresponde a la unidad deseada (paso 1), se debe asegurar que sea la tarjeta que se desea formatear (paso 2) y al final se debe cliquear en **Kill** (paso 3)

**Formateo de tarjeta MicroSD**

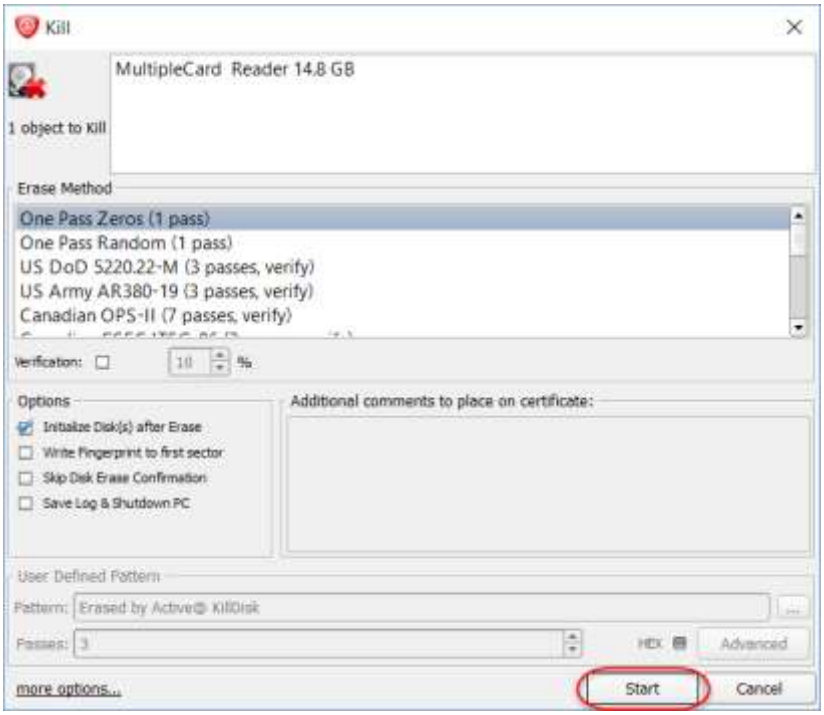


**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

A continuación, se selecciona el botón **Start**:

**Inicio de proceso de formateo de tarjeta MicroSD**

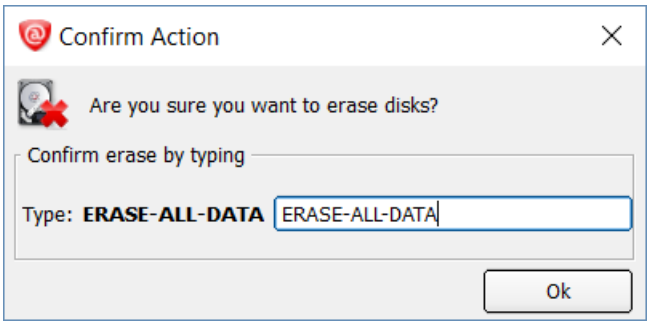



**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

Antes de empezar a dar formato, el programa realiza una última validación y se solicita ingresar la frase **ERASE-ALL-DATA** y luego presionar OK para iniciar el proceso; tardará varios minutos dependiendo de la capacidad de la tarjeta de memoria.

**Confirmación de borrado de tarjeta MicroSD**



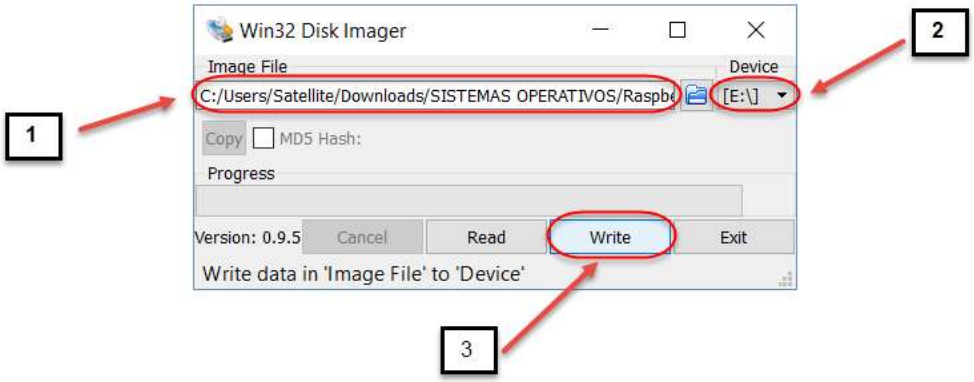

**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

**Carga de la imagen ISO del Sistema Operativo a la tarjeta de memoria**

Para proceder con la carga del sistema operativo, se debe utilizar el programa **Win32 Disk Imager**, luego se debe seleccionar la localidad de la imagen ISO (paso 1), escoger la unidad que se asignó para la tarjeta de memoria (paso 2) y presionar el botón **Write** (paso 3)**:**

**Carga de imagen ISO**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

Luego de haberse cargado la imagen del sistema operativo a la tarjeta de memoria, se procede a quitar la tarjeta microSD del adaptador e introducirla en la ranura de la Raspberry Pi.

**Instalación del servidor OpenVPN en Raspbian**

Previo a la instalación debemos proceder a asignar automáticamente una IP mediante asignación por MAC ADDRESS en el Firewall de la empresa; también se debe realizar la redirección de paquetes a un puerto especificado. En este caso para la realización de pruebas se realizó con el puerto 1194 UDP.

**Asignación IP Estática por MAC Address**


**Fuente:** Datos del proyecto

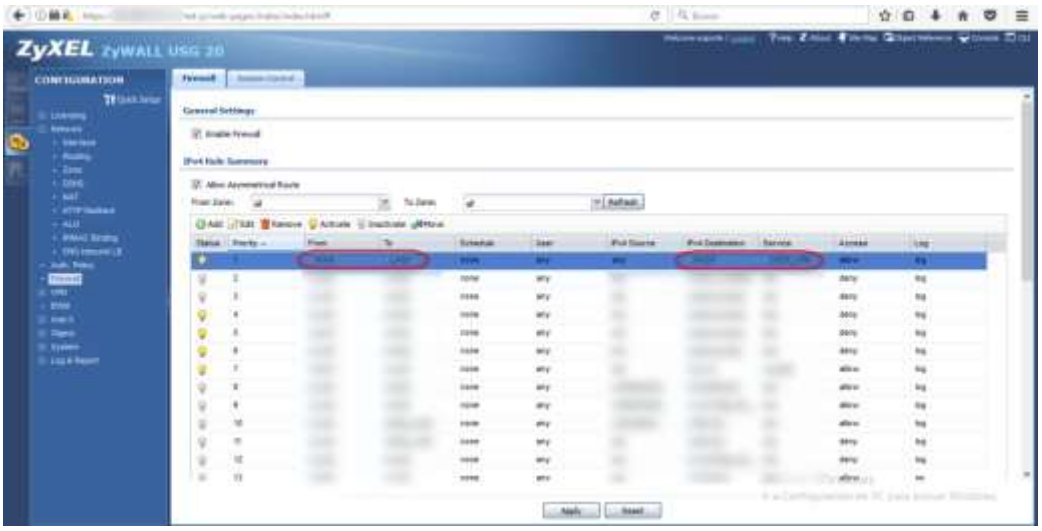
**Elaboración:** Edwin Sánchez Estrada

**Creación de regla de direccionamiento de puertos**


**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

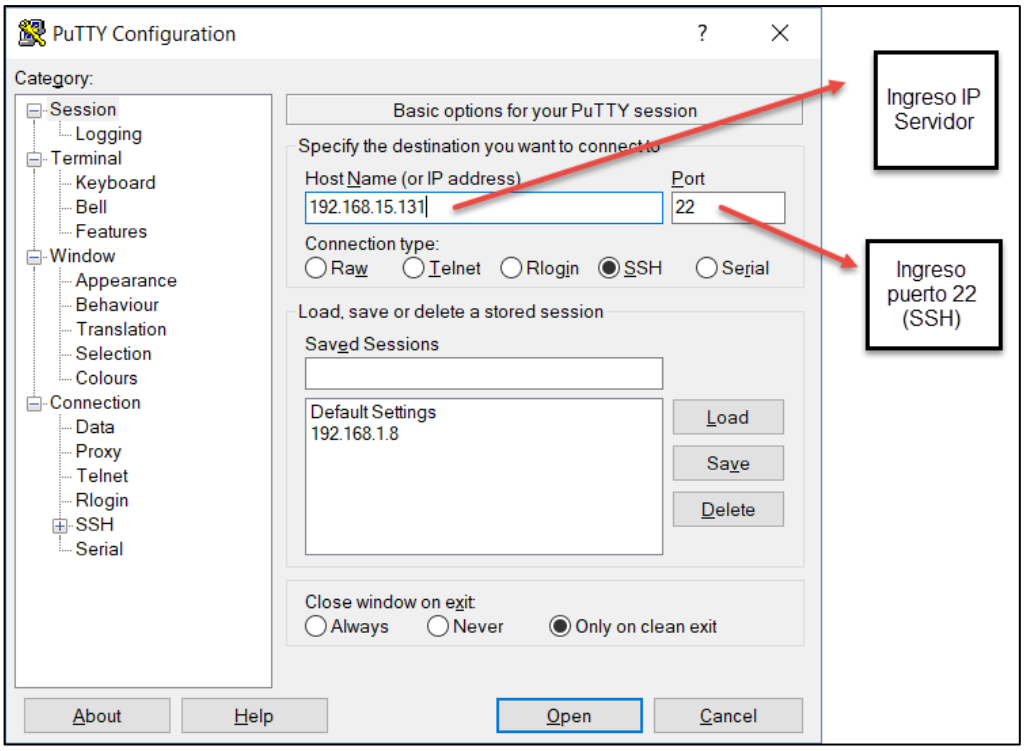
**Creación de regla de OpenVPN en Firewall**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

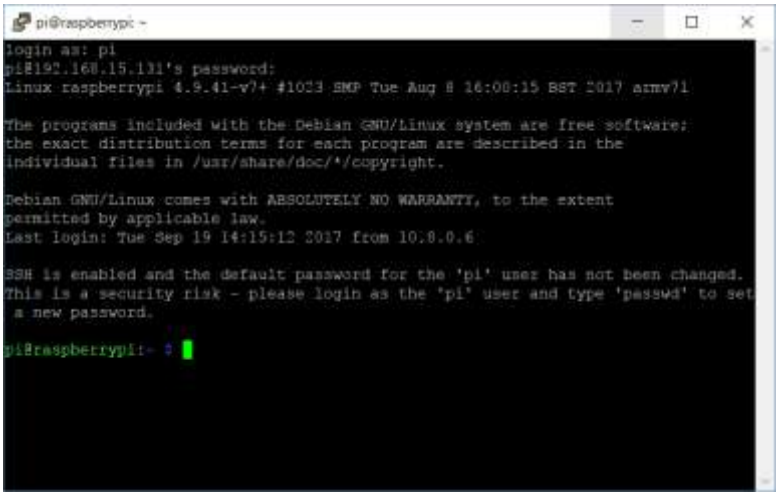
**Ingreso al servidor mediante aplicativo Putty**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

**Ingreso al Servidor mediante SSH**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

Las credenciales de ingreso inicial son:

**Usuario:** pi

**Contraseña:** raspberry

Se sugiere realizar el cambio por temas de seguridad, por lo cual se utilizará el comando ***passwd*** y luego pedirá el ingreso de la nueva clave.

```
pi@raspberry:~$ passwd
```

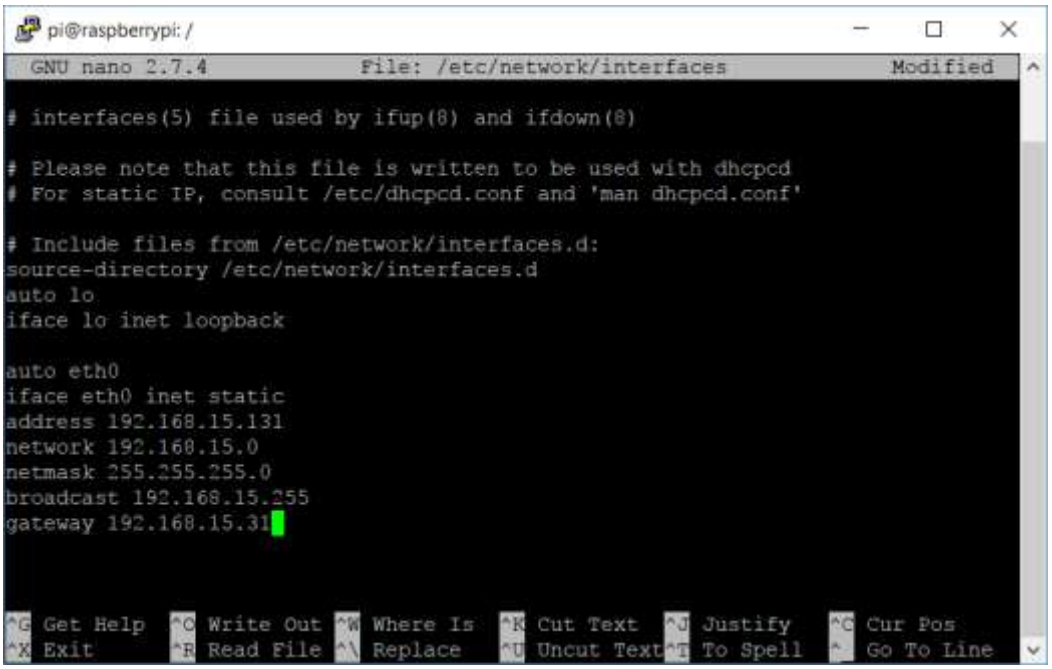
El cambio de contraseña nos permitirá realizar posteriores ingresos mediante SSH con este usuario sin privilegios.

### Creación de Ip estática en el servidor

En el apartado anterior se realizó la asignación de Ip estática desde el firewall, sin embargo, es necesario proceder a realizar la configuración también dentro del servidor para que la conexión VPN función de manera adecuada, para ello procederemos a ingresar en la siguiente ruta ***/etc/network*****,** editaremos el archivo con el comando ***nano*****.**

```
pi@raspberry:~$ sudo nano /etc/network/interfaces
```

**Ingreso al Servidor mediante SSH**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

Una vez realizada esta configuración podremos realizar la actualización del sistema operativos y también al upgrade del mismo. Lo realizaremos con los siguientes comandos.

```
pi@raspberry:~$ sudo apt-get update
pi@raspberry:~$ sudo apt-get upgrade
```

Luego de realizada la actualización se procede con la instalación del servidor OpenVPN.

```
pi@raspberry:~$ sudo apt-get install openvpn
```

Se debe confirmar la instalación digitando ‘s’ o ‘y’, según sea el caso. Una vez instalado se procede a realizar la generación de claves y certificados digitales.

**Generación de certificados digitales y claves del servidor.**

Se procederán a realizar la generación de claves públicas y privadas RSA para cifrado y firmas digitales; para este fin utilizaremos la siguiente instrucción.

```
pi@raspberry:~$ sudo su
pi@raspberry:~# cp -r /usr/share/easy-rsa /etc/openvpn/easy-rsa
```

De esta manera copiaremos el contenido del directorio ***/usr/share/easy-rsa*** en la carpeta ***/etc/openvpn/easy-rsa*** de forma recursiva y tendremos los datos originales en la carpeta inicial en caso de algún inconveniente futuro.

Luego procedemos a editar el archivo ***vars*** donde se cambiarán algunos parámetros que permitirán la creación de los certificados antes mencionados, para ello primero debemos cambiar de directorio a ***/etc/openvpn/easy-rsa*** y luego proceder con la modificación.

```
pi@raspberry:~# cd /etc/openvpn/easy-rsa
pi@raspberry:~# nano vars
```

Se debe proceder a cambiar la configuración y debe quedar como el presente archivo:

```
# easy-rsa parameter settings

# NOTE: If you installed from an RPM,
# don't edit this file in place in
# /usr/share/openvpn/easy-rsa --
# instead, you should copy the whole
# easy-rsa directory to another location
# (such as /etc/openvpn) so that your
# edits will not be wiped out by a future
# OpenVPN package upgrade.

# This variable should point to
# the top level of the easy-rsa
# tree.
export EASY_RSA="/etc/openvpn/easy-rsa"

#
# This variable should point to
# the requested executables
#
export OPENSSL="openssl"
export PKCS11TOOL="pkcs11-tool"
export GREP="grep"


# This variable should point to
# the openssl.cnf file included
# with easy-rsa.
export KEY_CONFIG=$EASY_RSA/openssl-1.0.0.cnf #

# Edit this variable to point to
# your soon-to-be-created key
# directory.
#
# WARNING: clean-all will do
# a rm -rf on this directory
# so make sure you define
# it correctly!
export KEY DIR="$EASY RSA/keys"

# Issue rm -rf warning
echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY DIR

# PKCS11 fixes
export PKCS11 MODULE PATH="dummy"
export PKCS11_PIN="dummy"

# Increase this to 2048 if you
```

```
# are paranoid.  This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export KEY_SIZE=2048

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"

# X509 Subject Field
export KEY_NAME="EasyRSA"

# PKCS11 Smart Card
# export PKCS11_MODULE_PATH="/usr/lib/changeme.so"
# export PKCS11_PIN=1234

# If you'd like to sign all keys with the same Common Name, uncomment the
KEY_CN export below
# You will also need to make sure your OpenVPN server config has the
duplicate-cn option set
# export KEY_CN="CommonName"
```

Se procede a guardar presionando ***Ctrl+X***, luego consultará si se está seguro de guardar los cambios, se oprime ***'y'***; luego ***Entrar***. Con esto ya habremos procedido a indicar que la longitud de clave a utilizar será de 256 bits y la ruta donde se encuentra la variable EASY_RSA.

Procedemos con la generación del certificado CA y root CA, manteniendo el prompt en el directorio ***/etc/openvpn/easy-rsa*** y para ello se procede a digitar las siguientes líneas de instrucción:

```
pi@raspberry:/etc/openvpn/easy-rsa# source ./vars
```

Este comando permite cargar el archivo ***vars*** anteriormente creado; aparecerá un mensaje que menciona que en caso de digitar la línea ***./clean-all*** se procerá a borrar el contenido del directorio ***/etc/openvpn/easy-rsa/keys***. Como es la primera vez procedemos a utilizar dicho ejecutable.

```
pi@raspberry:/etc/openvpn/easy-rsa# ./clean-all
```

Luego de borrar los datos del directorio ***keys*** procedemos a crear el certificado utilizando el ejecutable ***./build-ca***; después nos consultará datos adicionales correspondientes a la configuración del servidor. Se ingresarán los datos que a continuación se resaltan.

```
Country name (2 letter code) [US]: EC
State or Province Name (full name) [CA]: GY
Locality Name (eg, city) [San Francisco]: Guayaquil
Organization Name (eg, company) [Fort-Funston]: Reporne
Organizational Unit Name (eg, section)[MyOrganizationalUnit]:
Universidad_Guayaquil
Common Name (eg, your name or your server's hostname) [Fort-Funston]:
repornevpn
Name [vpn-server]: repornevpn
Email Address [email]: vguerrero@reporne.com.ec
```

Luego de crear el certificado digital, se procede a brindar un nombre al servidor donde se solicitará colocar los mismos datos anteriores. Se deben colocar iguales y luego pedirá firmar el certificado y confirmarlo, por ende, colocaremos ***'y'*** cuando lo solicite.

```
pi@raspberry:/etc/openvpn/easy-rsa# ./build-key-server repornevpn
```

**Generación de claves para los clientes.**

De esta manera ya se tiene el servidor configurado y está listo para crear certificados para cliente, para ello utilizaremos el comando ***./build-key-pass <usuario>***. En el campo usuario, digitaremos el deseado. Se adjunta un ejemplo con el usuario ***jalonso***

Esto permitirá la creación del usuario dentro del servidor y el archivo de configuración requerido para la comunicación entre el host que tendrá instalado el cliente y el server OpenVPN de manera segura mediante el túnel de Datos.

**Generación de certificado para cliente**


**Fuente:** Datos del proyecto

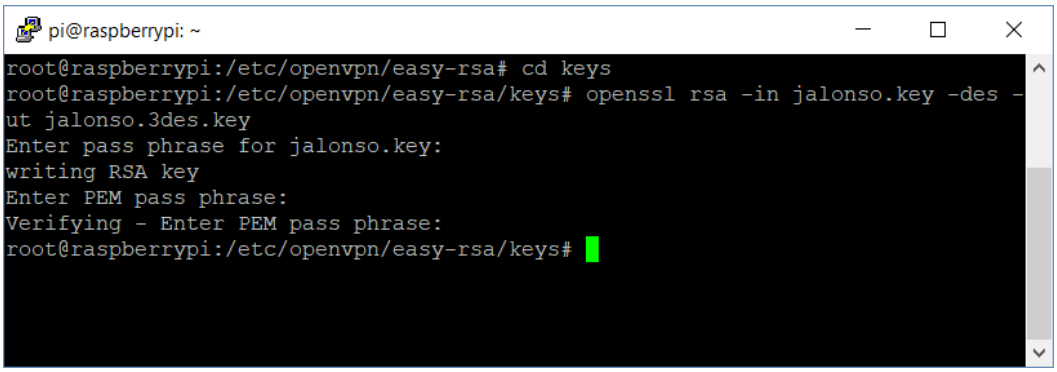
**Elaboración:** Edwin Sánchez Estrada

Se procede a utilizar el algoritmo de encriptación 3DES, mediante la herramienta OpenSSL incorporada; pedirá la contraseña ingresada en el paso anterior, por lo cual se la debe digitar las veces que se solicite.

Antes, se debe cambiar al directorio ***/etc/openvpn/easy-rsa/keys*** y luego se ejecuta el siguiente script:

```
pi@raspberry:/etc/openvpn/easy-rsa# cd keys
pi@raspberry:/etc/openvpn/easy-rsa/keys# openssl rsa -in jalonso.key -des -out
jalonso.3des.key
```

**Encriptación por algoritmo 3DES**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

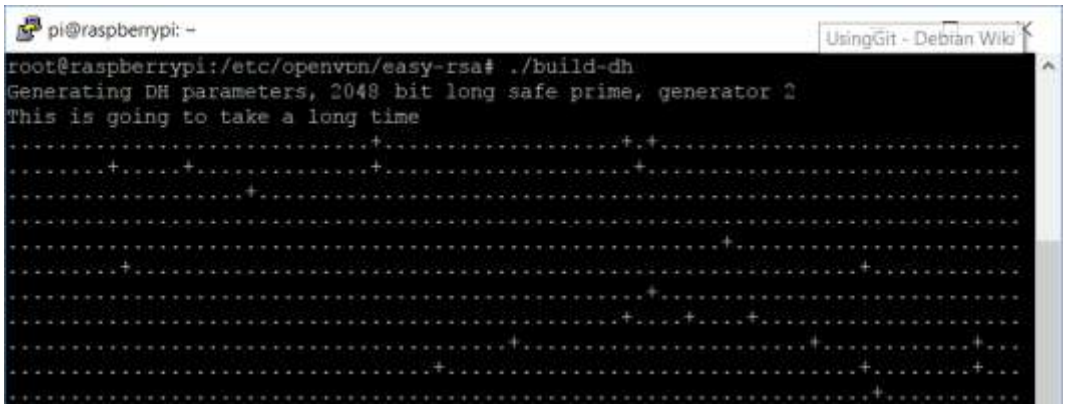
Una vez que se ha generado los certificados de cliente, se procede a ejecutar el script para generación de intercambio de claves de dos entidades desconocidas, ***Diffie-Hellman***, permitiendo la utilización de un servidor público para este propósito. Para ello, se debe cambiar de directorio a la carpeta ***/etc/openvpn/easy-rsa***.

```
pi@raspberry:/etc/openvpn/easy-rsa/keys# cd ..
pi@raspberry:/etc/openvpn/easy-rsa# ./build-dh
```

Al iniciar la ejecución del script ***./build-dh*** comienza la generación aleatoria de claves mediante un algoritmo matemático que incluye la

exponenciación. Su seguridad se basa en lo dificultoso de calcular en un cuerpo finito, logaritmos discretos. Debido a su longitud de 2048 bits, esta tarea tardará entre 15 a 20 minutos.

**Generación de clave de 2048 bits**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

**Parámetros de configuración adicionales para el servidor.**

El servidor VPN es vulnerables a ataques de denegación de servicios, por lo cual se procederá a blindarlo para evitar esta falla de seguridad, para ello ejecutaremos el siguiente script:

```
pi@raspberry:/etc/openvpn/easy-rsa # openvpn --genkey --secret keys/ta.key
```

Para que existe la comunicación adecuada para la conversación entre el servidor y los clientes, debe existir la ruta parametrizada, por lo cual, debemos crear un nuevo fichero con esta información. Se debe acceder a la ruta ***/etc/openvpn*** y alojaremos un archivo con el nombre ***server.conf***

```
pi@raspberry:/etc/openvpn/easy-rsa # cd ..
pi@raspberry:/etc/openvpn # nano server.conf
```

En el nuevo archivo, que estará en blanco, se debe pegar la siguiente información:

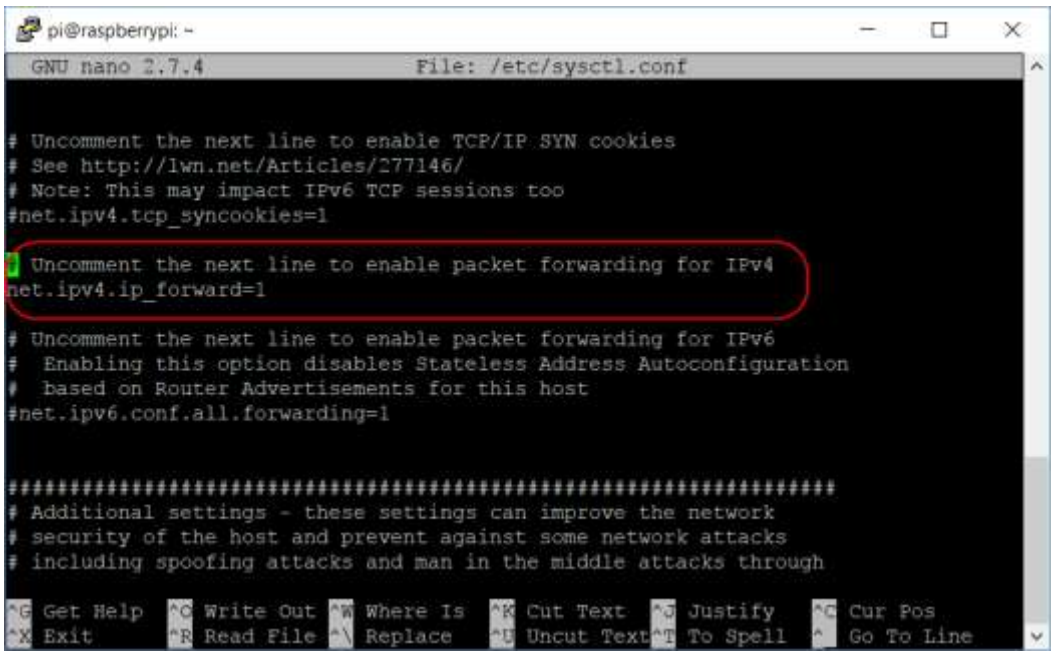
```
# local 192.168.15.131 # CAMBIAR ESTE NUMERO CON LA DIRECCIÓN IP DE TU
RASPBERRY
dev tun
proto udp #PUEDES DEJARLO ASI O CAMBIARLO A TCP
port 1194
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/repornevpn.crt # CAMBIA CON EL NOMBRE DE
TU CRT
key /etc/openvpn/easy-rsa/keys/repornevpn.key # CAMBIAR CON EL NOMBRE DE
TU KEY
dh /etc/openvpn/easy-rsa/keys/dh2048.pem # PUEDE CAMBIARLO A 1024 SI
DESEAS
server 10.8.0.0 255.255.255.0
# server and remote endpoints
ifconfig 10.8.0.1 10.8.0.2
# Add route to Client routing table for the OpenVPN Server
push "route 10.8.0.1 255.255.255.255"
# Add route to Client routing table for the OpenVPN Subnet
push "route 10.8.0.0 255.255.255.0"
# your local subnet
push "route 192.168.15.131 255.255.255.0" # CAMBIAR CON LA IP DEL
RASPBERRY
# Set primary domain name server address to the SOHO Router
# If your router does not do DNS, you can use Google DNS 8.8.8.8
push "dhcp-option DNS 8.8.8.8" # This should already match your router
address and not need to be changed.
# Override the Client default gateway by using 0.0.0.0/1 and
# 128.0.0.0/1 rather than 0.0.0.0/0. This has the benefit of
# overriding but not wiping out the original default gateway.
push "redirect-gateway def1"
client-to-client
duplicate-cn
keepalive 10 120
tls-auth /etc/openvpn/easy-rsa/keys/ta.key 0
cipher AES-128-CBC
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn-status.log 20
log /var/log/openvpn.log
verb 1
```

Los campos en verde, deben ser cambiados según la configuración del servidor que se esté configurando. Después se presiona ***Ctrl + X***, se confirma y guarda digitando ***'y'*** las veces que solicita, al final ***Enter.***

El servidor no redirecciona el tráfico de internet por defecto, por lo cual se debe modificar el archivo ***/etc/sysctl.conf*** y descontentar un parámetro para este fin. Luego de ello, para confirmar y aplicar los cambios con éxito, se debe ejecutar la línea ***sysctl -p***

```
pi@raspberry:/etc/openvpn # nano /etc/sysctl.conf
```

**Habilitación de redireccionamiento de tráfico**



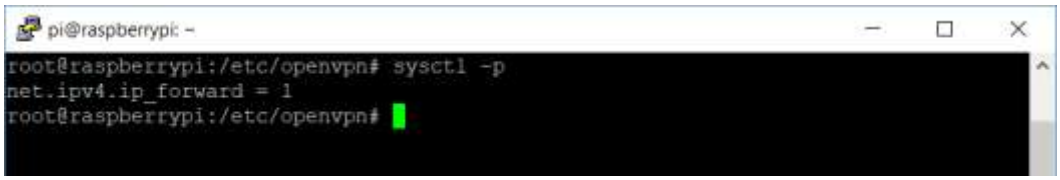

**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

```
pi@raspberry:/etc/openvpn # sysctl -p
```

Al ingresar este comando se le envía la orden al Kernel del Sistema operativo para la modificación de configuración en tiempo de ejecución y se envía la petición de cargar el archivo con las modificaciones realizadas.

**Carga de modificación de redireccionamiento.**




**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Ahora ya está el servidor listo, con las configuraciones cargadas y los certificados de cliente y servidor creados, pero aún no se podrá tener comunicación debido a que existe en Linux un firewall incorporado el cual bloquea las conexiones entrantes. Habilitar todos los permisos no es una buena práctica debido a la inseguridad que provoca, por ello se procederá a crear una regla que se cargará cada vez que se encienda el equipo. Dentro del directorio ***/etc/*** crearemos un archivo con nombre ***firewall-openvpn-rules.sh***

```
pi@raspberry:/etc/openvpn # cd ..
pi@raspberry:/etc # nano firewall-openvpn-rules.sh
```

Dentro del archivo en mención, se incluirá lo siguiente:

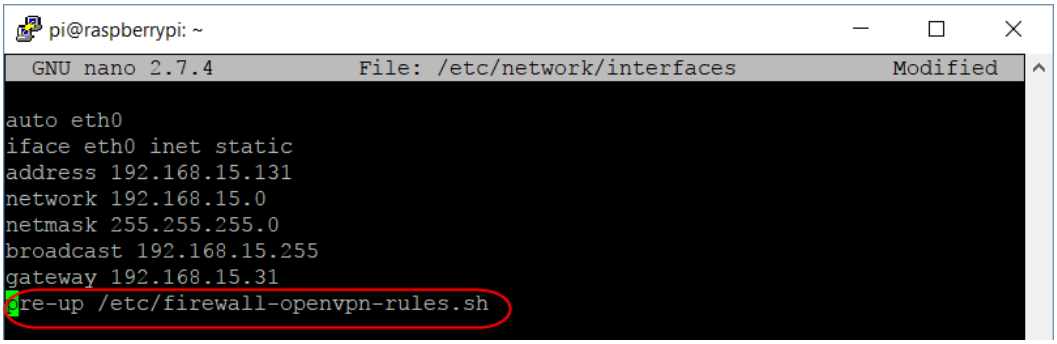
```
#!/bin/sh
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j SNAT --to-source
192.168.15.131
```

**-j SNAT** → indicador que menciona que el tráfico proviene de una IP con NAT.
**eth0** → corresponde a la interfaz de red Ethernet
**192.168.15.131** → IP del servidor configurado

Se procede a dar permisos de ejecución al nuevo archivo creado mediante la línea de comando ***chmod 700 /etc/firewall-openvpn-rules.sh*** y luego se cambia del propietario actual a root: ***chown root /etc/firewall-openvpn-rules.sh***. Para que este script se ejecute en cada inicio del sistema, agregaremos la ruta en el archivo ***network/interfaces*** para este fin.

```
pi@raspberry:/etc/openvpn # chmod 700 /etc/firewall-openvpn-rules.sh
pi@raspberry:/etc/openvpn # chown root /etc/firewall-openvpn-rules.sh
pi@raspberry:/etc/openvpn # nano /etc/network/interfaces
```

**Ingreso de reglas de firewall**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

Al final, se realiza el reseteo del servidor con el comando ***sudo reboot*** para que los cambios tengan efecto.

**Configuración del cliente OpenVPN**

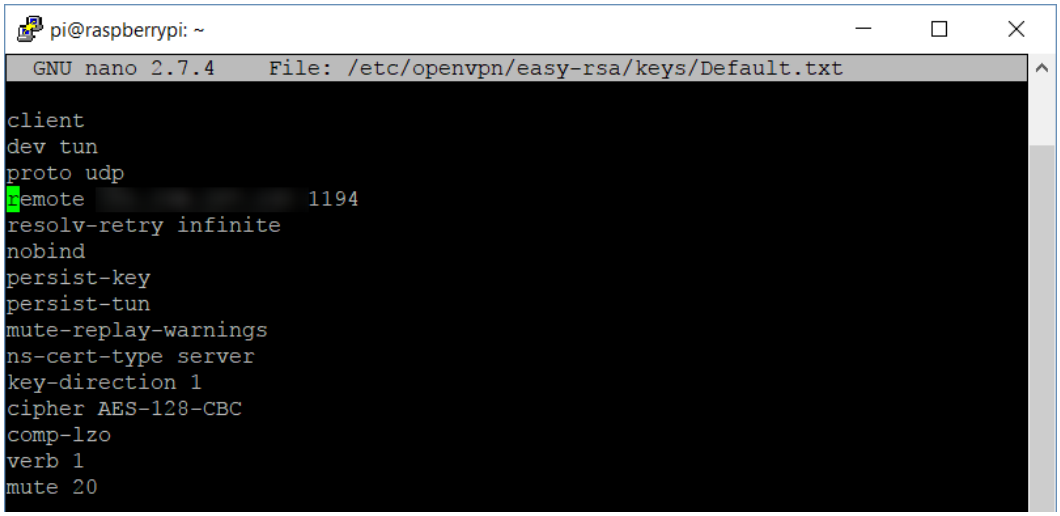
Con los pasos anteriores, se realizó la creación de una clave distinta para cada dispositivo que va a interactuar con el servidor VPN levantado, sin embargo, para que pueda ser configurado en los clientes se deben generar los archivos de configuración respectivos empleando un script previamente desarrollado por Eric Jodoin, del instituto SANS.

Se gestionará la creación de un nuevo fichero en la ruta ***/etc/openvpn/easy-rsa*** llamado ***Default.txt*** en el cual deberemos colocar

la IP pública a utilizar. En este caso, por temas de seguridad de la empresa **no** será visible dicha dirección.

```
pi@raspberry:/etc/openvpn # nano /etc/openvpn/easy-rsa/keys/Default.txt
```

**Creación de archivo Default.txt**




**Fuente:** Datos del proyecto

**Elaboración:** Edwin Sánchez Estrada

Se debe proceder a crear el script que ayudará a automatizar la creación del archivo de configuración para los clientes OpenVPN. Al fichero a crear estará en el directorio ***/etc/openvpn/easy-rsa/keys*** y será nombrado ***MakeOVPN.sh***; estas instrucciones fueron creadas también por Eric Jodoin.

```
pi@raspberry:/etc/openvpn # nano /etc/openvpn/easy-rsa/keys/MakeOVPN.sh
```

En este fichero, se debe alojar el siguiente grupo de instrucciones:

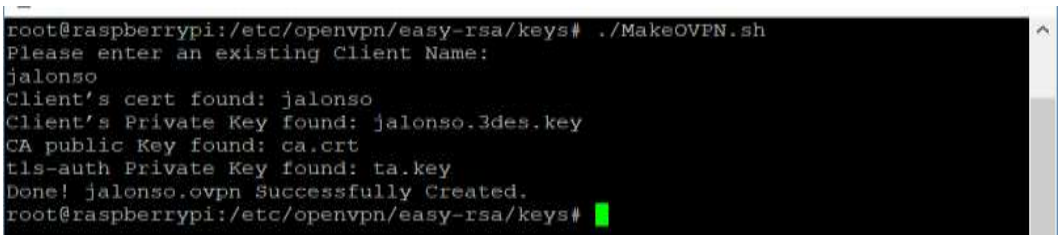
```
#!/bin/bash

# Default Variable Declarations
DEFAULT="Default.txt"
FILEEXT=".ovpn"
CRT=".crt"
KEY=".3des.key"
CA="ca.crt"
TA="ta.key"

#Ask for a Client name
echo "Please enter an existing Client Name:"
read NAME


#1st Verify that client's Public Key Exists
if [ ! -f $NAME$CRT ]; then
 echo "[ERROR]: Client Public Key Certificate not found: $NAME$CRT"
 exit
fi
echo "Client's cert found: $NAME$CR"


#Then, verify that there is a private key for that client
if [ ! -f $NAME$KEY ]; then
 echo "[ERROR]: Client 3des Private Key not found: $NAME$KEY"
 exit
fi
echo "Client's Private Key found: $NAME$KEY"

#Confirm the CA public key exists
if [ ! -f $CA ]; then
 echo "[ERROR]: CA Public Key not found: $CA"
 exit
fi
echo "CA public Key found: $CA"

#Confirm the tls-auth ta key file exists
if [ ! -f $TA ]; then
 echo "[ERROR]: tls-auth Key not found: $TA"
 exit
fi
echo "tls-auth Private Key found: $TA"

#Ready to make a new .opvn file - Start by populating with the default
file
cat $DEFAULT > $NAME$FILEEXT

#Now, append the CA Public Cert
echo "<ca>" >> $NAME$FILEEXT
cat $CA >> $NAME$FILEEXT
echo "</ca>" >> $NAME$FILEEXT
```

```
#Next append the client Public Cert
echo "<cert>" >> $NAME$FILEEXT
cat $NAME$CRT | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >>
$NAME$FILEEXT
echo "</cert>" >> $NAME$FILEEXT

#Then, append the client Private Key
echo "<key>" >> $NAME$FILEEXT
cat $NAME$KEY >> $NAME$FILEEXT
echo "</key>" >> $NAME$FILEEXT

#Finally, append the TA Private Key
echo "<tls-auth>" >> $NAME$FILEEXT
cat $TA >> $NAME$FILEEXT
echo "</tls-auth>" >> $NAME$FILEEXT

echo "Done! $NAME$FILEEXT Successfully Created."

#Script written by Eric Jodoin
#\ No newline at end of file
```

Debido a que el directorio ***keys*** se encuentra solo con permisos de lectura, se procede a modificarlos a fin de poder ejecutar el script recientemente creado.

```
pi@raspberry:/etc/openvpn # cd /etc/openvpn/easy-rsa/keys
pi@raspberry:/etc/openvpn/easy-rsa/keys # chmod 700 MakeOVPN.sh
pi@raspberry:/etc/openvpn/easy-rsa/keys # ./MakeOVPN.sh
```

**Ejecución de script ./MakeOVPN.sh**




**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Estos pasos se deberán seguir cada vez que se desee crear un cliente nuevo en el servidor.

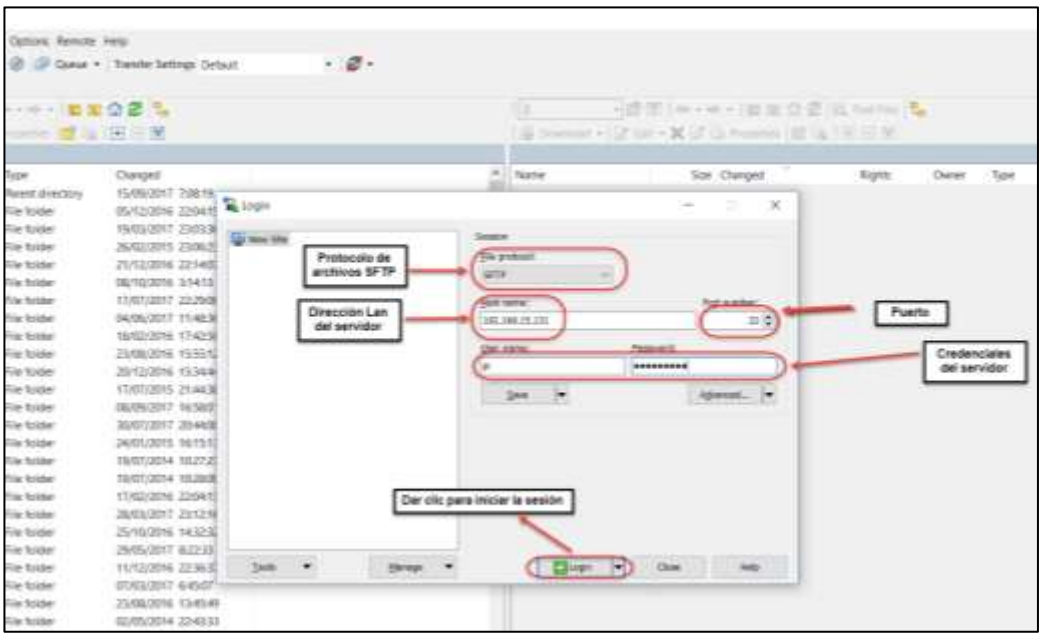
**Descarga de archivos de configuración desde el servidor**

Para proceder con la configuración del cliente, debemos obtener los archivos de configuración previamente creados; para ellos utilizaremos el software **WinSCP**. Sin embargo, antes debemos dar permisos a la carpeta ya que no dará opción a visualizarlos en primera instancia; ejecutamos el siguiente comando.

```
pi@raspberry:/etc/openvpn # chmod 700 -R /etc/openvpn
```

Con el programa WinSCP se realizará la conexión hacia el servidor mediante el protocolo SFTP

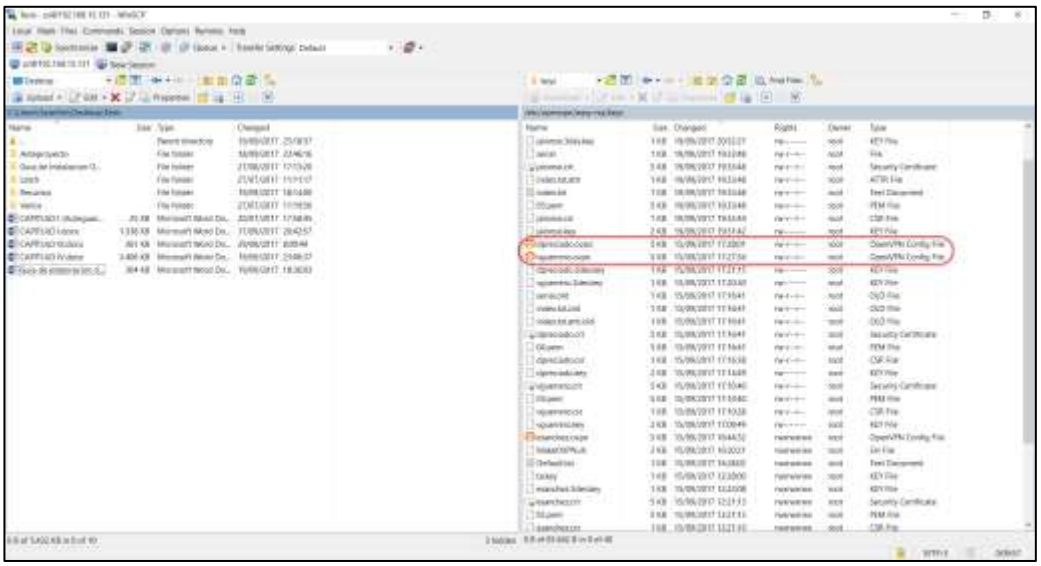
**Ingreso al Servidor herramienta WinSCP**




**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Una vez ingresada las credenciales, se procede a tomar los archivo con extensión ***.OVPN*** los cuales servirán para que el host pueda negociar con el servidor para su posterior conexión VPN.

**Ruta de archivos .ovpn en servidor**



**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Luego de que se hayan copiados todos los archivos necesarios para alojarlos en los N clientes que pudiesen existir, se debe volver a dar permisos solo de lectura para evitar que algún atacante tenga acceso al mismo

```
pi@raspberry:/etc/openvpn # chmod 600 -R /etc/openvpn
```

### Integración de Latch con el servidor OpenVPN

Para la integración de Latch, se debe proceder a descargar el plugin necesario dentro del servidor mediante la ejecución del siguiente comando:

```
pi@raspberry:~$ wget https://github.com/ElevenPaths/latch-plugin-unix/archive/master.zip
```

**Descarga de plugin Latch**


**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Se realiza la extracción del paquete y luego a la instalación con las siguientes líneas:

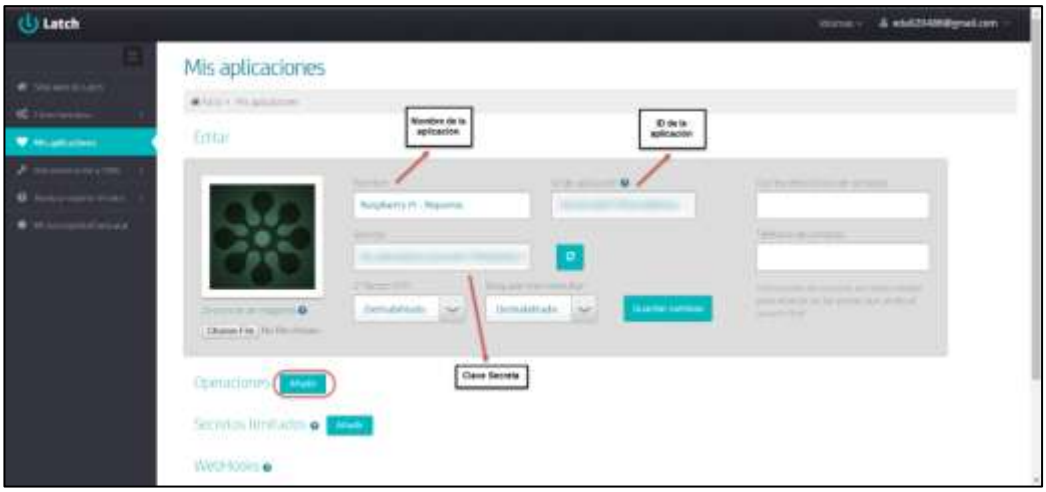
```
pi@raspberry:~$ unzip master.zip
pi@raspberry:~$ cd latch-plugin-unix-master/
```

```
pi@raspberry:~/latch-plugin-unix-master $ ./configure prefix=/usr
sysconfdir=/etc && make && sudo make install
```

Una vez instalado el plugin, se procede con la configuración del pareo del servicio. Antes de ello, debemos crear una cuenta en la página https://latch.elevenpaths.com/www/, en la sección ***Registrarse como desarrollador***, allí se ingresarán los datos necesarios en el formulario y la activación de la cuenta mediante el correo electrónico.

Con las credenciales creadas, procedemos a iniciar sesión y nos situamos en la opción ***Añadir una nueva aplicación*;** solicitará el ingreso de un nombre, para este proyecto se colocará ***Raspberry PI – Reporne***

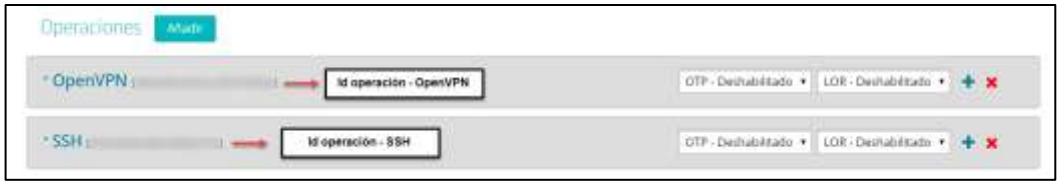
**Administración de aplicaciones Latch**




**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Dentro de ***Operaciones*** se da clic en el botón ***añadir*** para proceder a crear los servicios ***OpenVPN*** y ***SSH***.

**Creación Id operaciones OpenVPN y SSH**




**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Con estos datos previamente creados, se realizará la integración con el servidor OpenVPN, para esto, se debe ingresar a la aplicación instalada en el celular del administrador de la red, donde se generará el token de aplicación.

**Generación de Token en APP Móvil Latch**


**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

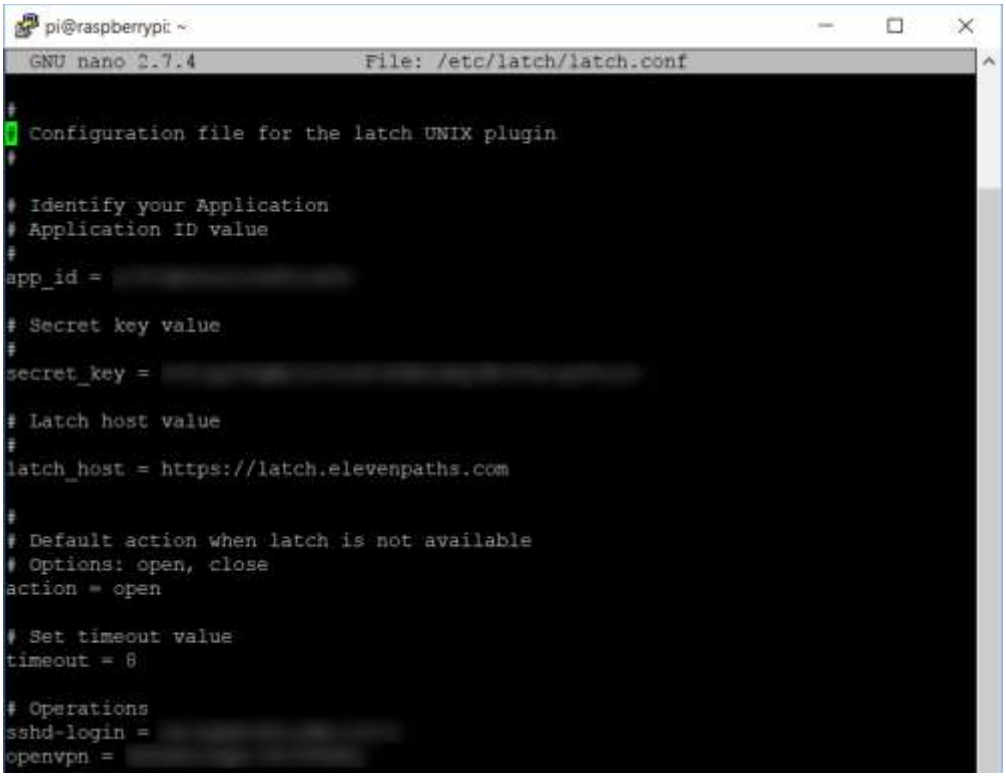
Este token, es ingresado vía comando al servidor para proceder con el pareo de la aplicación y el servidor.

```
pi@raspberry:~# latch -p EW4FeT
```

Luego del pareo, se procede con la configuración del servicio Latch dentro del servidor, para ello se debe acceder al archivo de configuración correspondiente donde se pondrán los datos generados inicialmente:

```
pi@raspberry:~# nano /etc/latch/latch.conf
```

**Archivo de configuración Latch**




**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

Debido a que se está trabajando en un ambiente Unix, se debe realizar la autenticación mediante PAM, para ellos debemos acceder al directorio ***/lib/arm-linux-gnueabihf/security*** por lo cual debemos mover los archivos de configuración de Latch a la carpeta en mención mediante el siguiente comando:

```
pi@raspberry:~# mv /usr/lib/pam_latch.so /lib/arm-linux-gnueabihf/security
```

El archivo de configuración del servicio SSH se lo podrá encontrar en ***/etc/pam.d/sshd***, para vincular este servicio, se debe adicionar la siguiente línea al fichero en mención:

```
auth required pam_latch.so config=/etc/latch/latch.conf accounts=/
etc/latch/latch.accounts operation=sshd-login otp=no
```

El archivo de autenticación PAM para el caso de OpenVPN se encuentra en la ruta ***/usr/lib/openvpn/openvpn-plugin-auth-pam.so***, se debe crear un servicio en el directorio ***/etc/pam.d*** con el nombre ***openvpn*** y se deberá incluir allí lo siguiente:

```
auth required pam_latch.so config=/etc/latch/latch.conf accounts=/
etc/latch/latch.accounts operation=openvpn otp=no
```

En el caso del servidor OpenVPN donde se ha creado una capa adicional de seguridad, se añadirá lo siguiente al archivo ***server.conf***

```
plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so openvpn
```

A los archivos de configuración de los clientes (.ovpn), se les agregará la siguiente línea:

```
auth-user-pass
```

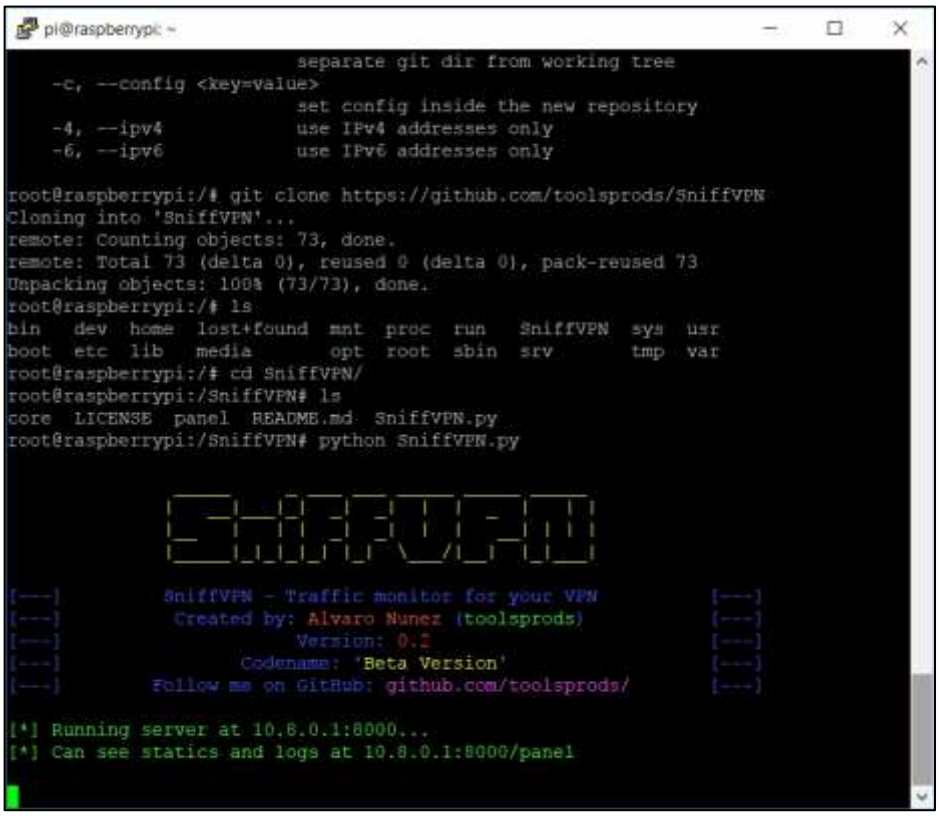
Luego, se debe reiniciar el servidor para que los cambios generados se apliquen correctamente.

### Instalación e integración del servicio SniffVPN

Para proceder con la instalación de este servicio adicional gratuito, se deben ejecutar las siguientes líneas de código:

```
pi@raspberry:~# git clone https://github.com/toolsprods/SniffVPN
pi@raspberry:~# cd SniffVPN
pi@raspberry:~# python SniffVPN.py
```

**Servicio SniffVPN iniciado**




**Fuente:** Datos del proyecto
**Elaboración:** Edwin Sánchez Estrada

## ANEXO N ° 5

## Acta de aceptación del proyecto

REPORNE S.A.

Facilito
Red de servicios

Guayaquil, 19 de septiembre del 2017

**Sres.**
**Universidad de Guayaquil**
**Ciudad.**

Por medio de la presente confirmó la aceptación del proyecto realizado por el Sr. EDWIN EDUARDO SÁNCHEZ ESTRADA, con C.I. 092315959-4, estudiante de la Carrera de Ingeniería en Networking y Telecomunicaciones, de la Facultad de Ciencias Matemáticas y Física; iniciado el 19 de junio del presente año, cumpliendo con las siguientes actividades:

- Servidor VPN montado en Raspberry Pi, implementado.
- Manual técnico de configuración
- Manual de usuario para clientes
- Página que permite visualizar el tráfico de los usuarios en la VPN.

Atentamente

**Víctor Guerrero Zambrano**
**Líder de Infraestructura**
**Reporne S.A.**

General Córdova 808 y Víctor Manuel Rendón Edif. Torres de la Merced, Piso 14 Of. 4 - Telef.: 04-2328400

## ANEXO N ° 6

## Manual de usuario

### Descarga del cliente OpenVPN

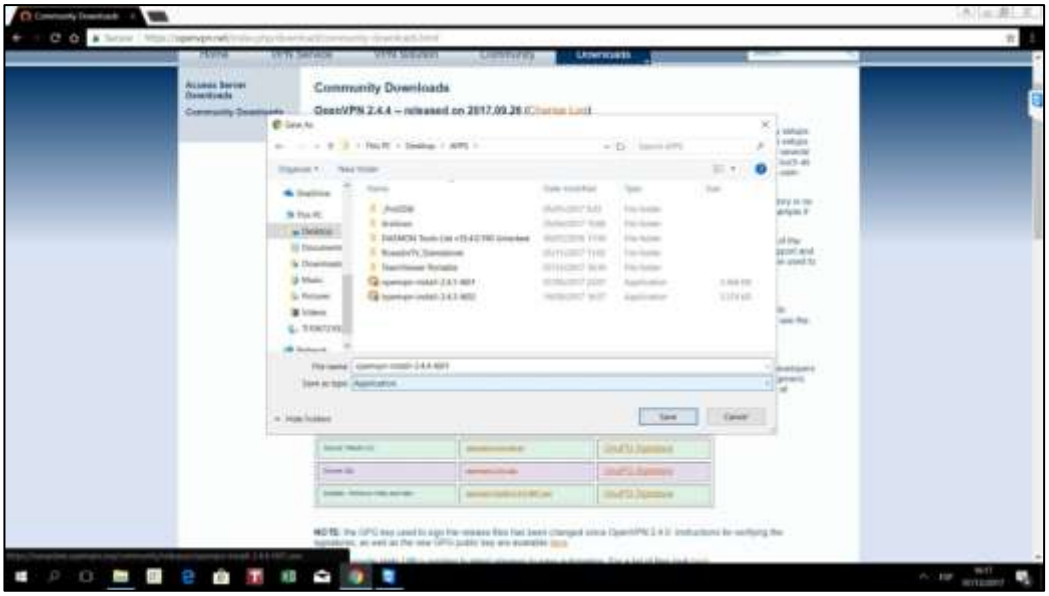
Para poder establecer una conexión VPN mediante OpenVPN se requiere la instalación del cliente en el host remoto.

Para este fin, se debe descargar la aplicación en la siguiente dirección https://openvpn.net/, luego se selecciona la opción ***Community***.


Luego, en el menú Downloads seleccionamos ***Community Donwloads***

Luego seleccionamos la versión más reciente según el sistema operativo requerido.


Una vez seleccionado, procedemos a guardar el archivo ejecutable.

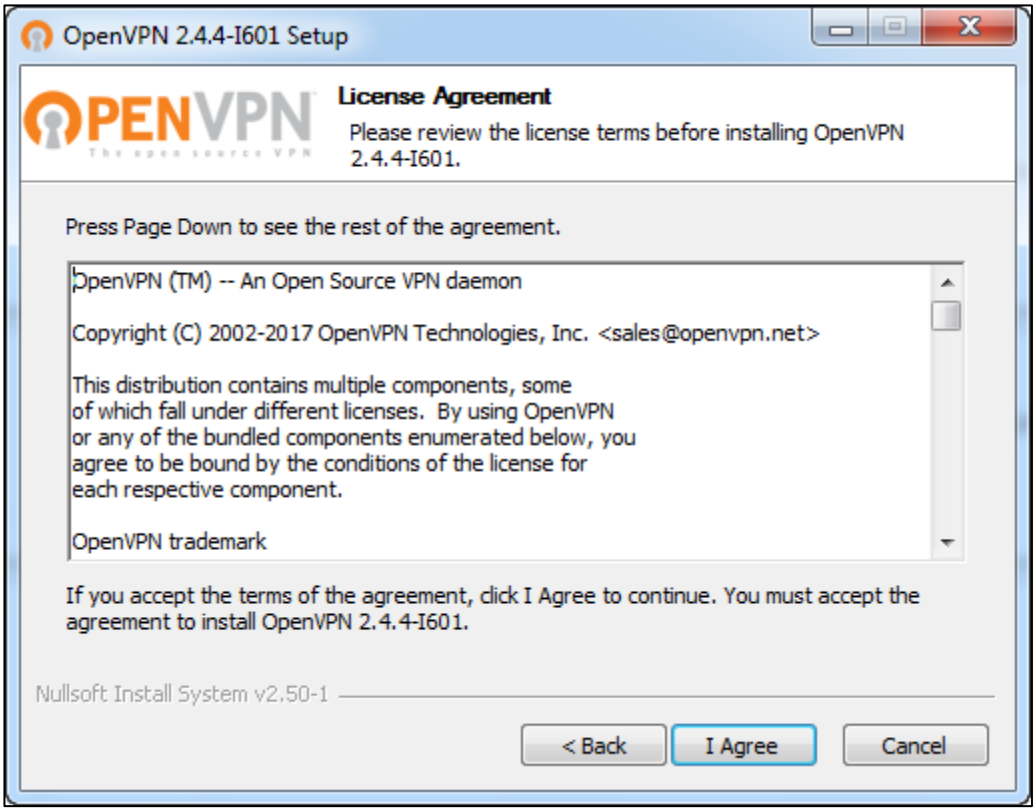


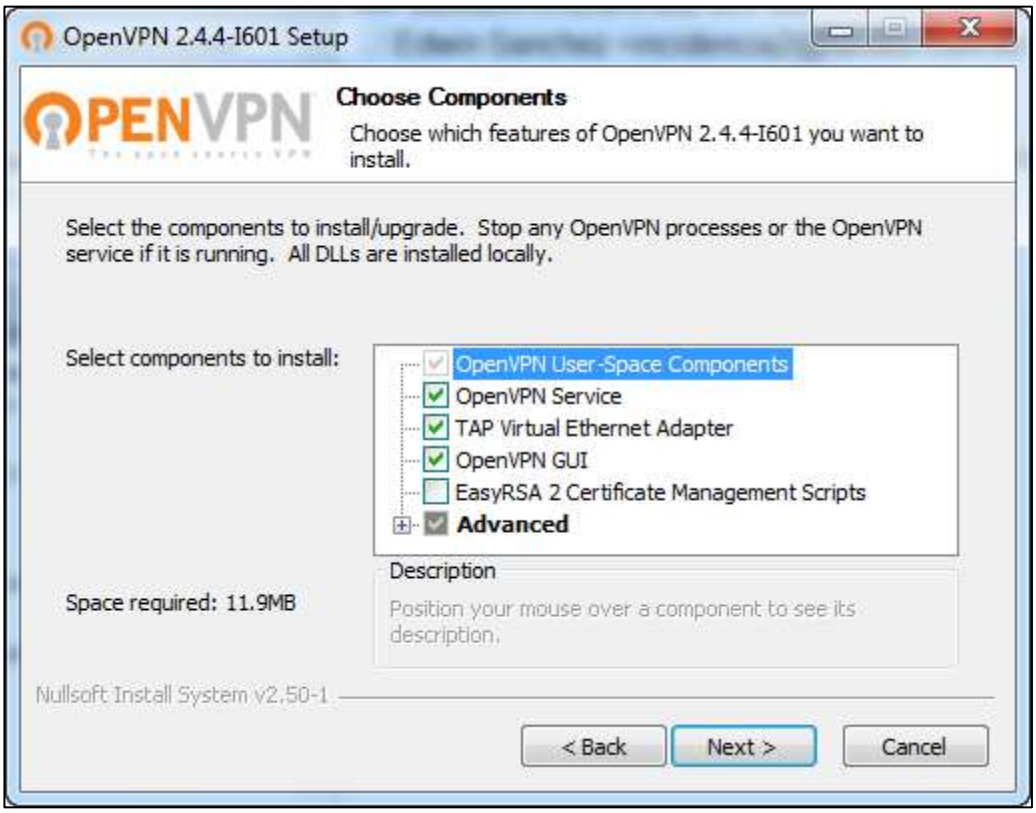
**Instalación del cliente OpenVPN**

Una vez descargado, se ejecuta la aplicación y se sigue el proceso dando clic en “next” o “siguiente”.

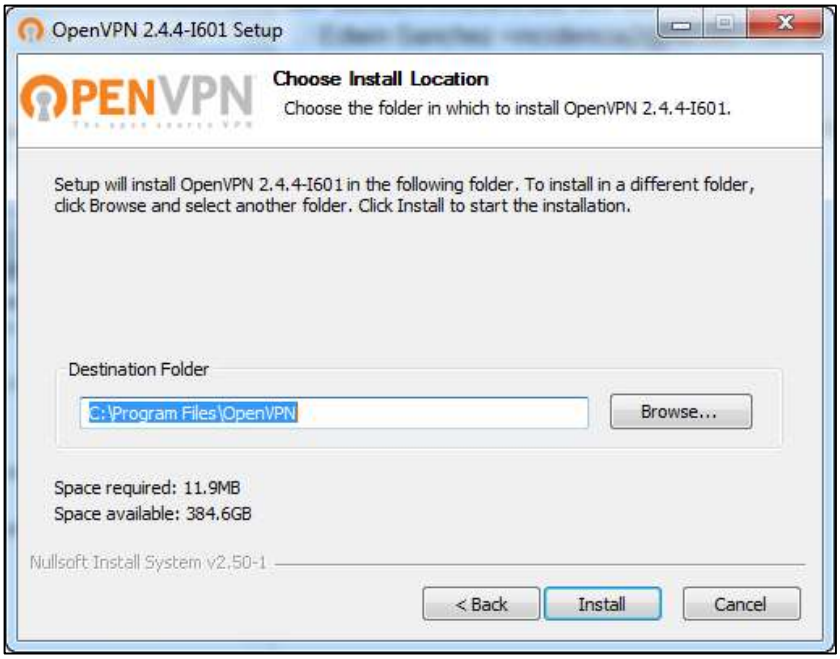

Se procede a aceptar los términos y condiciones y se eligen los componentes que se requieren.

Se sugiere dejar los valores por defecto para evitar algún problema posterior en el funcionamiento por falta de compatibilidad

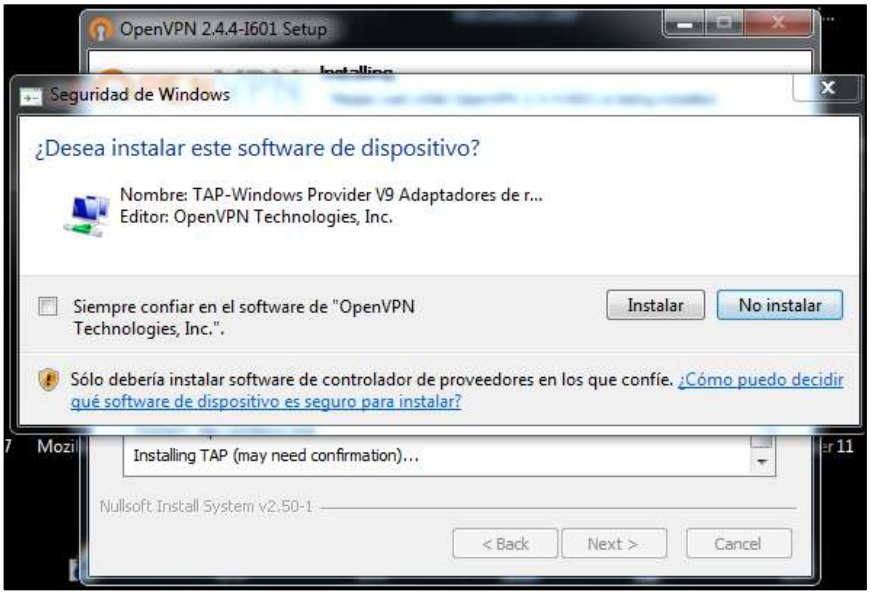

OpenVPN 2.4.4-I601 Setup
License Agreement
Please review the license terms before installing OpenVPN 2.4.4-I601.
Press Page Down to see the rest of the agreement.
OpenVPN (TM) -- An Open Source VPN daemon
Copyright (C) 2002-2017 OpenVPN Technologies, Inc. <sales@openvpn.net>
This distribution contains multiple components, some
of which fall under different licenses. By using OpenVPN
or any of the bundled components enumerated below, you
agree to be bound by the conditions of the license for
each respective component.
OpenVPN trademark
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.4.4-I601.
Nullsoft Install System v2.50-1
< Back
I Agree
Cancel


OpenVPN 2.4.4-I601 Setup
Choose Components
Choose which features of OpenVPN 2.4.4-I601 you want to install.
Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.
Select components to install:
OpenVPN User-Space Components
OpenVPN Service
TAP Virtual Ethernet Adapter
OpenVPN GUI
EasyRSA 2 Certificate Management Scripts
Advanced
Description
Position your mouse over a component to see its description.
Space required: 11.9MB
Nullsoft Install System v2.50-1
< Back
Next >
Cancel

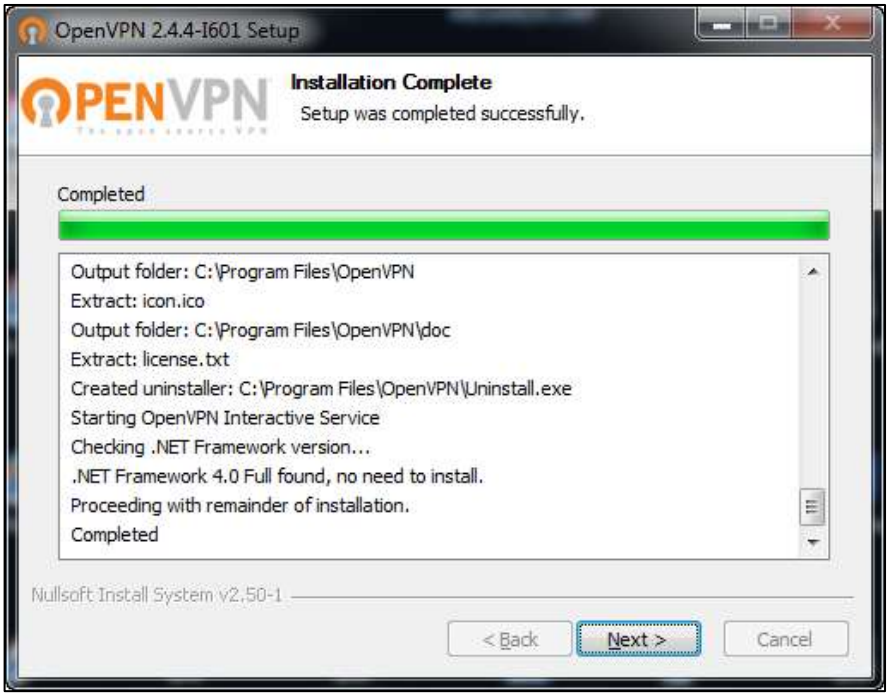
Se debe poner atención cuando aparezca la ruta donde se vaya a instalar la aplicación, puesto que se requerirá luego para los certificados del servidor.

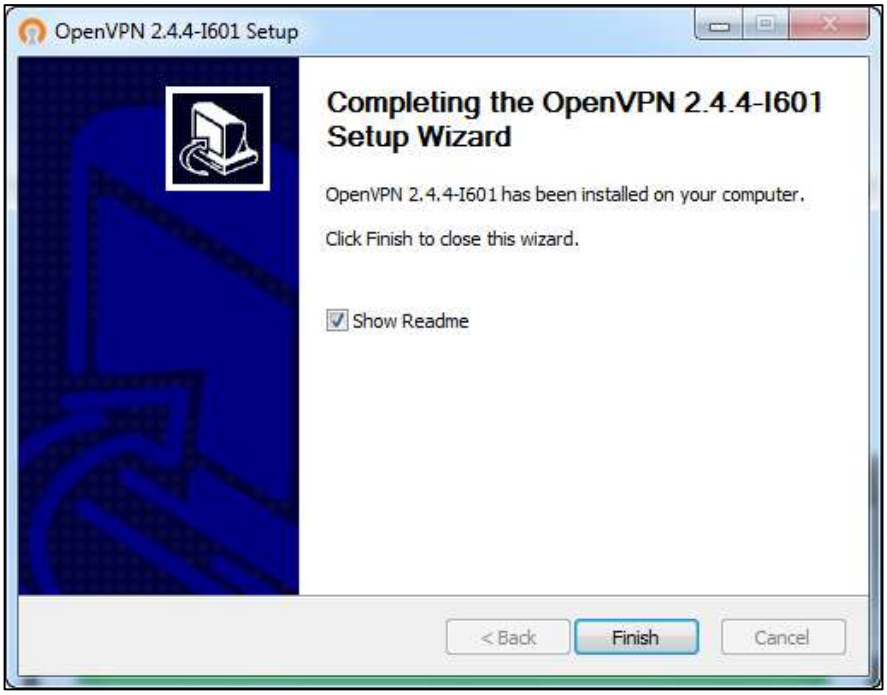



Aparecerá un mensaje consultando si deseamos instalar el controlador TAP a lo que pondremos ***instalar***.



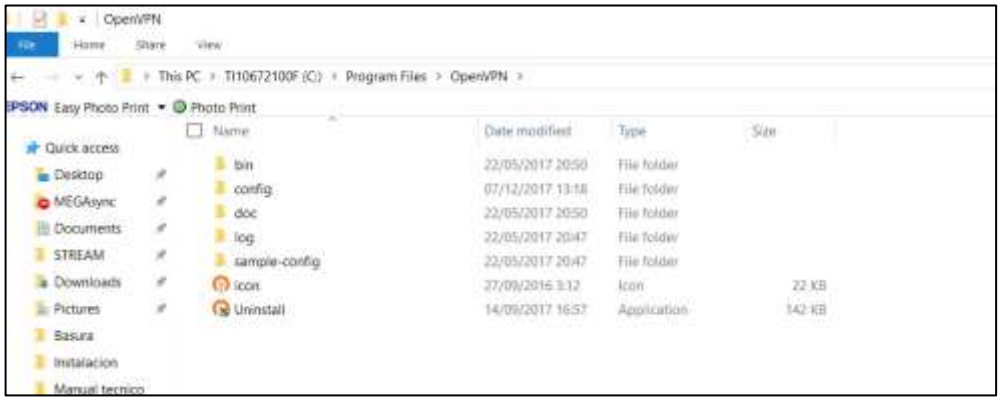
Luego de que aparezca que la instalación se ha completado, se procede a dar clic en **next** y luego en **Finish** con ello quedará instalado el servicio.



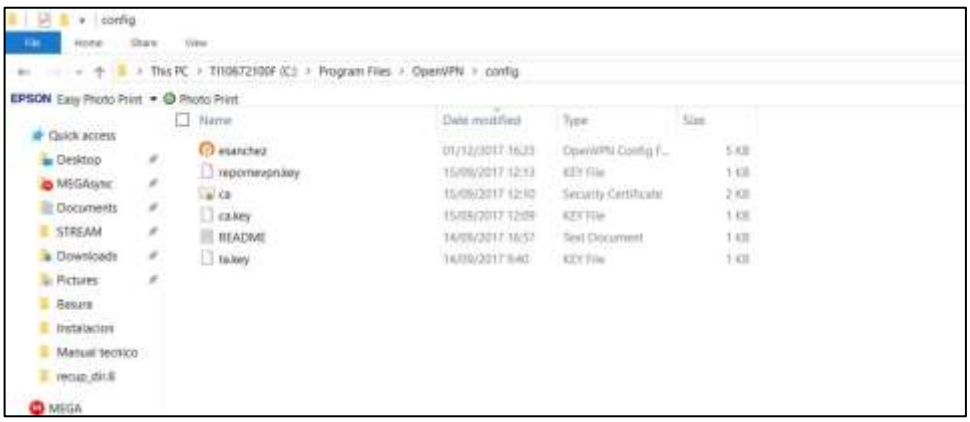
**Uso del cliente OpenVPN**

Para poder utilizar el cliente, procederemos primero a ubicar la carpeta donde se realizó la instalación, para este caso será **C:\Program Files\OpenVPN**

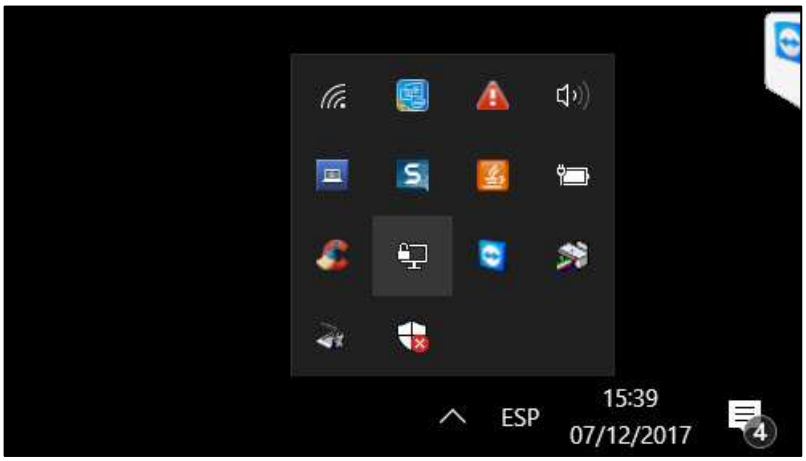



Procederemos a pegar los archivos de configuración del servidor y el archivo de configuración del cliente .OVPN. Para este manual, serán los siguientes:

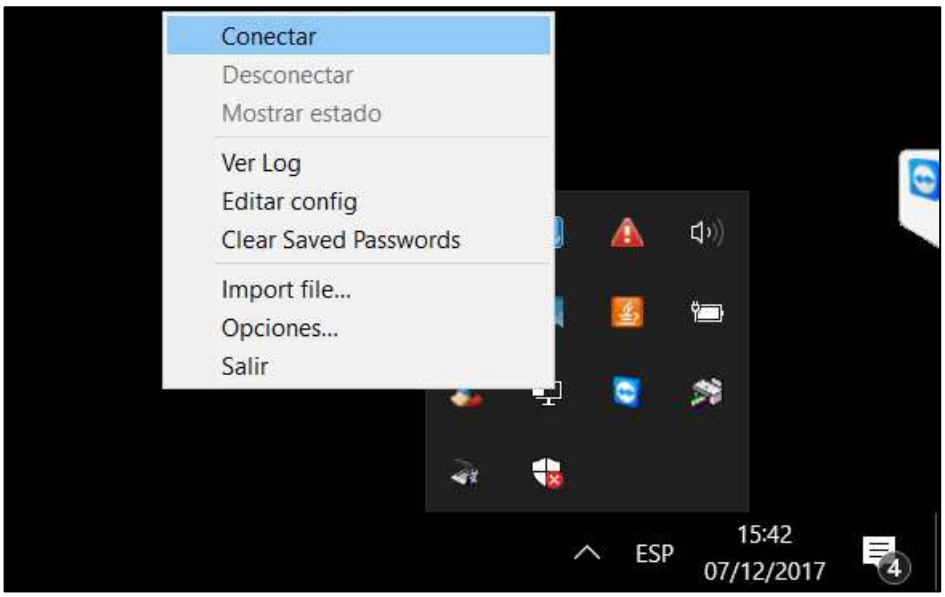
- **esanchez.ovpn**
- **ca.crt**
- **reporne.key**
- **ca.key**
- **ta.key**



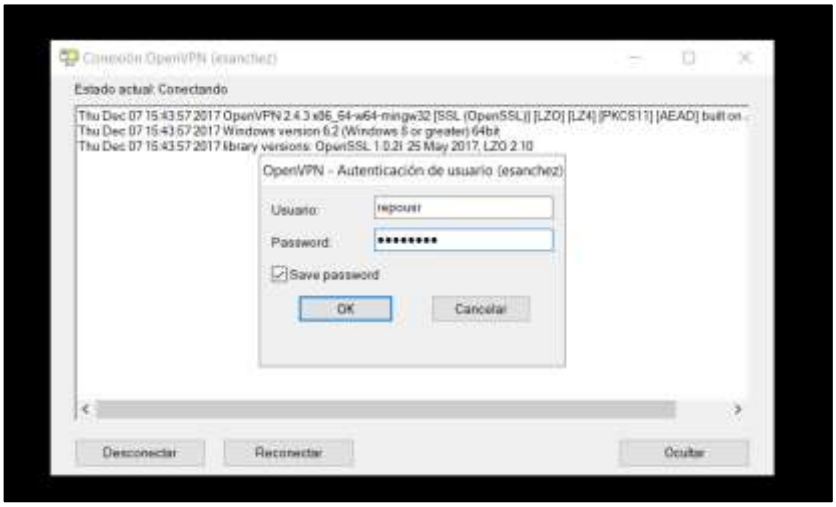
Dentro de los iconos ocultos en la barra de tareas, podremos encontrar un PC con un candado (icono de OpenVPN); procedemos a dar clic derecho en el mismo.



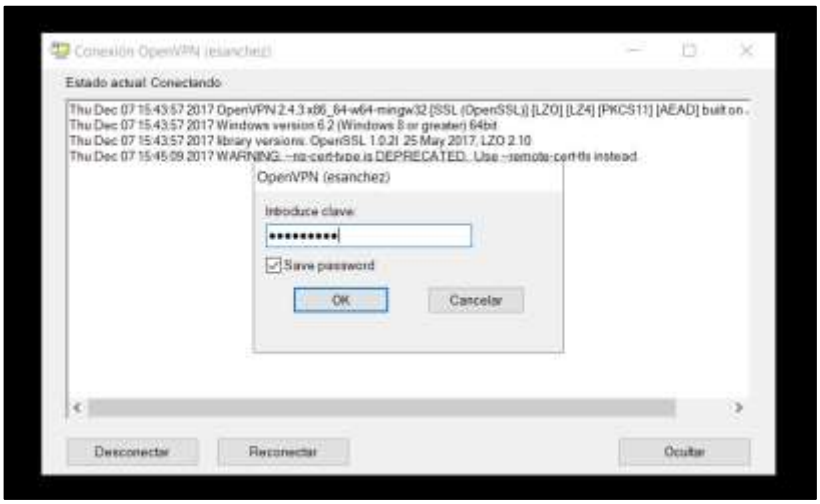

Damos clic en ***Conectar*** donde luego nos pedirá datos adicionales para el ingreso al servicio.




Debido a que se encuentra configurada la petición de credenciales, se deberá ingresar el usuario y contraseña configurado en UNIX (Servidor).




Se coloca la clave del archivo de configuración .OVPN




Con esto, el túnel VPN de datos se encuentra establecido y podrá acceder a la red LAN configurada.